OLIVIER BOSSARD • MAUD RIVIÈRE

LA GRANDE AVENTURE DU BITCOIN ET DE LA BLOCKCHAIN

octopus

LA GRANDE AVENTURE DU BITCOIN ET DE LA BLOCKCHAIN

SCÉNARIO
OLIVIER BOSSARD

DESSIN ET COULEUR
MAUD RIVIÈRE

DELCOURT

SOMMAIRE

CHAPITRE 1 – **INTRODUCTION AU BITCOIN**
Du troc au Bitcoin
La publication du *Livre blanc du Bitcoin*
Qui était Satoshi Nakamoto ?
Qui sont les cypherpunks ?
La naissance du premier bitcoin !
Comment les bitcoins sont-ils émis ?
Comment Bitcoin contrôle-t-il son offre ?
Pourquoi est-il encore possible de miner des bitcoins ?
En quoi Bitcoin est-il différent des jetons d'achat comme les Q Coins ?
Deux pizzas à plus de 100 millions de dollars !
Le successeur de Nakamoto, Gavin Andresen
Le « robinet aux bitcoins »
Quelles politiques gouvernementales envers les cryptos ?

CHAPITRE 2 – **LE BITCOIN EN PRATIQUE**
Comment fonctionnent les transactions en bitcoins ?
Que se passe-t-il lors d'une transaction Bitcoin ?
Quels frais pour les transactions Bitcoin ?
Qu'est-ce qu'un nœud Bitcoin ?
La signature numérique Bitcoin
Quelques précisions sur l'envoi de bitcoins

CHAPITRE 3 – **LE PROCESSUS DE MINAGE**
Le minage en pratique
Qui sont les mineurs ?
Qu'est-ce qu'une *mining rig* ?
L'évolution des plateformes de minage Bitcoin
À quoi ressemble une ferme de minage ?
Qu'est-ce qu'un *pool* de minage ?
Qu'est-ce que la capacité de hachage ?
Qu'est-ce que la comptabilité concurrentielle ?

CHAPITRE 4 – **LE BITCOIN COMME VÉHICULE D'INVESTISSEMENT**
Quels outils pour investir dans les crypto-actifs ?
Comment utiliser une plateforme d'échange ?
Comment fonctionne le trading de gré à gré ?
Qu'est-ce que le trading quantitatif ?
Qu'est-ce qu'une plateforme d'échange décentralisée ?
Pourquoi utiliser un portefeuille Bitcoin ?
Cold wallet et *hot wallet*
Les nœuds complets et les portefeuilles en ligne
Puis-je utiliser des jetons bitcoin comme moyen de paiement ?
Comment échanger des crypto-monnaies entre elles ?

CHAPITRE 5 – **LA TECHNOLOGIE BLOCKCHAIN**
L'histoire de la technologie *blockchain*
Blockchain, « la machine de confiance »
Comment fonctionne la *blockchain* ?
Qu'est-ce qu'un horodatage ?
Comment la *blockchain* fait-elle consensus ?
Comment catégorise-t-on les *blockchains* ?

CHAPITRE 6 – **MÉCANISMES DE CONSENSUS ET BIFURCATIONS**
Qu'est-ce que le mécanisme de consensus par « preuve de travail » ?
Qu'est-ce que le mécanisme de consensus par « preuve d'enjeu » ?
Qu'est-ce que la « preuve d'enjeu déléguée » ?
Qu'est-ce que la « preuve à divulgation nulle de connaissance » ?
Qu'est-ce que l'algorithme de hachage ?
Qu'est-ce que la cryptographie asymétrique ?
Pourquoi Bitcoin doit-il se mettre à l'échelle ?
Qu'est-ce qu'une bifurcation de *blockchain* ?
Quelle différence entre une bifurcation mineure et une bifurcation majeure ?
Qu'est-ce qu'une attaque par relecture ?
La bifurcation entre Ethereum et Ethereum Classic

CHAPITRE 7 – **APPLICATIONS DE LA BLOCKCHAIN : LES CRYPTO-MONNAIES**
Qu'est-ce qu'une crypto-monnaie ?
Caractéristique #1 : la transnationalité
Caractéristique #2 : l'anonymat
Caractéristique #3 : le registre distribué
Caractéristique #4 : la non-réplicabilité
Qu'est-ce que le Litecoin ?
Qu'est-ce que le NEM ?
Qu'est-ce que le Dash ?
Qu'est-ce que le Monero ?
Qu'est-ce que le Zcash ?

CHAPITRE 8 – **APPLICATIONS DE LA BLOCKCHAIN : PLATEFORMES, TOKENISATION**
Qu'est-ce qu'une plateforme ?
Qu'est-ce que Ethereum ?
Qu'est-ce que EOS ?
Les jetons utilitaires
Qu'est-ce que le jeton utilitaire Augur ?
Qu'est-ce que le jeton utilitaire Golem ?
Les jetons d'actifs
Qu'est-ce que le jeton d'actifs Digix ?
Qu'est-ce que le jeton d'actifs USDT ?

CHAPITRE 9 – **POTENTIEL DE LA BLOCKCHAIN**
La *blockchain* peut-elle changer le monde comme Internet l'a fait ?
Quels sont les inconvénients de la *blockchain* ?
Les grandes organisations autour de la *blockchain*

CHAPITRE 1

INTRODUCTION AU BITCOIN

DU TROC AU BITCOIN

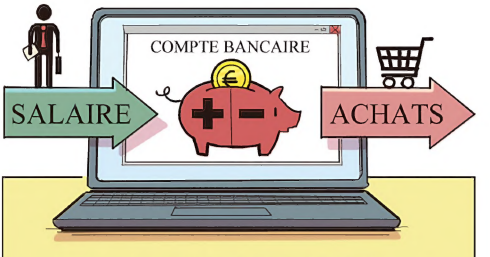
Autrefois, on utilisait en tant que monnaie d'échange des objets tels que des coquillages ou des pierres précieuses.

Leur rareté permettait d'en assurer la valeur.

On utilisa ensuite...

Autre bouleversement de la monnaie...

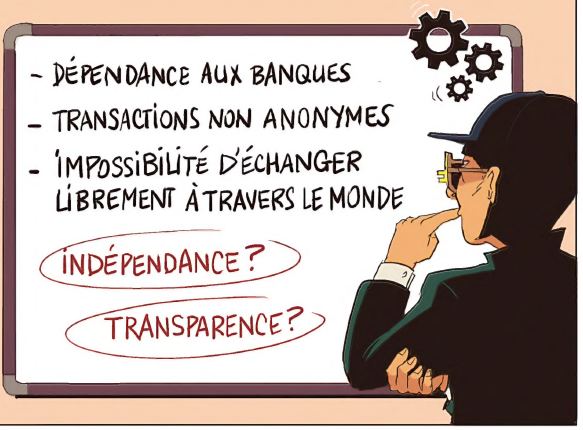
Avec Internet, nous sommes passés des billets de banque à des comptes dématérialisés...



... administrés UNIQUEMENT par les banques.

Un inconnu, caché sous le pseudonyme de Satoshi NAKAMOTO, refusa de subir cette dépendance aux banques centrales.

Il se mit à chercher un nouveau système de paiement qui répondrait aux problématiques soulevées par cette crise.



LA PUBLICATION DU LIVRE BLANC DU BITCOIN

En réponse à cette crise financière de 2008, ce mystérieux Satoshi NAKAMOTO publia un article en ligne intitulé...

« BITCOIN : UN SYSTÈME DE PAIEMENT ÉLECTRONIQUE ENTRE PARTICULIERS »*

Il y décrivait avec une précision redoutable le nouveau système de paiement électronique qu'il venait d'imaginer...

LE SYSTÈME BITCOIN.

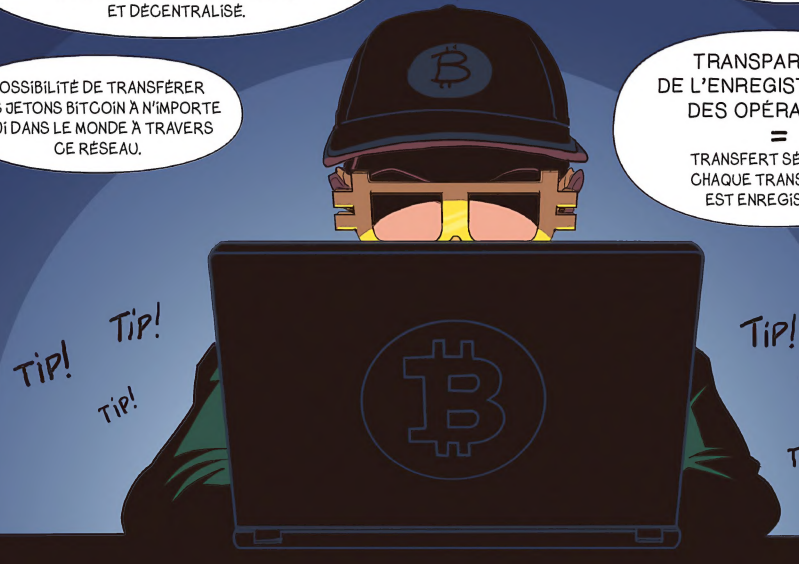
INDÉPENDANCE DU CONTRÔLE DE L'OFFRE DE MONNAIE
=
SYSTÈME MONÉTAIRE VIRTUEL POUVANT CONTRÔLER L'OFFRE ET L'ÉMISSION DES JETONS SANS AVOIR BESOIN D'AUCUNE AUTORITÉ CENTRALE.

... ÉMISSION DE JETONS APPELÉS DES BITCOINS.

DROIT ADMINISTRATIF POUR TOUS
=
SYSTÈME DE MONNAIE NUMÉRIQUE *PEER-TO-PEER* (DE PARTICULIER À PARTICULIER) ET DÉCENTRALISÉ.

POSSIBILITÉ DE TRANSFÉRER LES JETONS BITCOIN À N'IMPORTE QUI DANS LE MONDE À TRAVERS CE RÉSEAU.

TRANSPARENCE DE L'ENREGISTREMENT DES OPÉRATIONS
=
TRANSFERT SÉCURISÉ, CHAQUE TRANSACTION EST ENREGISTRÉE.



Bitcoin est donc à la fois le nom du système, de la technologie, et celui des jetons qui circulent dans ce système.

Véritable GENÈSE DU BITCOIN, ce *Livre blanc* marqua par sa publication la naissance de la technologie sous-jacente au Bitcoin...

LA FAMEUSE *BLOCKCHAIN*.

* Le texte original du *Livre blanc du Bitcoin* (11 pages en français) peut être téléchargé librement sur https://bitcoin.org/files/bitcoin-paper/bitcoin_fr.pdf. Il y est même traduit en 40 langues !

QUI ÉTAIT SATOSHI NAKAMOTO ?

Satoshi NAKAMOTO est le créateur et le développeur du système Bitcoin.

Il publia le *Livre blanc du Bitcoin* le 1er novembre 2008 et mina le tout premier jeton bitcoin le 3 janvier 2009.

Il devint ainsi la première personne capable d'utiliser ces jetons bitcoin, minés dans le fameux...

Je vous expliquerai bientôt en détail ce mécanisme de minage et de création des bitcoins.

MAIS QUI ÉTAIT RÉELLEMENT CE SATOSHI NAKAMOTO ?

Beaucoup de gens ont prétendu être cette personne.

2013

Certains émettent l'hypothèse que Satoshi NAKAMOTO est Shinichi MOCHIZUKI, un mathématicien de renommée mondiale.

JE SUIS BIEN SPÉCIALISTE DE LA THÉORIE DES NOMBRES. J'AI NOTAMMENT INTRODUIT LES FROBENIOÏDES, DÉVELOPPÉ LA THÉORIE DE TEICHMÜLLER INTER-UNIVERSELLE, ET AUSSI TENTÉ DE DÉMONTRER LA FAMEUSE CONJECTURE ABC...

... NÉANMOINS, JE NE SUIS PAS SATOSHI NAKAMOTO !

2014

Des pirates informatiques accèdent à l'adresse de messagerie de Satoshi NAKAMOTO et pensent découvrir que le propriétaire de ce compte est l'ingénieur Dorian NAKAMOTO.

MAIS PUISQUE JE VOUS DIS QUE C'EST UNE ERREUR !! J'AI OBTENU L'ACCÈS À CETTE ADRESSE ÉLECTRONIQUE ET SON MOT DE PASSE PAR HASARD !

2016

L'informaticien australien Craig WRIGHT crée un mauvais buzz en prétendant être le véritable Satoshi NAKAMOTO.

OUI, C'EST MOI ! ET JE PEUX LE PROUVER EN VOUS FOURNISSANT SA CLÉ PRIVÉE DE CRYPTAGE.

Cependant, WRIGHT dut retirer sa déclaration, n'étant même pas capable de répondre à tous les doutes exprimés.

Aujourd'hui, nous ne savons toujours pas qui est le réel Satoshi NAKAMOTO.

Il continue de cacher sa véritable identité, sans doute terrifié de l'impact que son invention pourrait avoir sur sa vie privée et sur sa sécurité.

ALLEZ, SI VOUS VOULEZ MON AVIS, JE PARIERAIS QU'IL S'AGIT EN FAIT D'UN GROUPE DE CYPHERPUNKS DE GÉNIE, PARMI LESQUELS...

QUI SONT LES CYPHERPUNKS?

Le *Livre blanc du Bitcoin* fut publié pour la première fois sur un réseau de messagerie chiffré appellé Cypherpunk.

CYPHER, EN ANGLAIS, DÉSIGNE UN MESSAGE CODÉ ET FAIT RÉFÉRENCE À CETTE BRANCHE DES MATHÉMATIQUES APPELÉE LA CRYPTOGRAPHIE.

VOUS SAVEZ, LE CODAGE ET LE DÉCODAGE SÉCURISÉ DE MESSAGES SECRETS.

Par extension, les utilisateurs de cette messagerie codée se font appeler les « cypherpunks ».

OUAÏP ! ON EST LES « PUNKS DE LA CRYPTOGRAPHIE ».

DES « VOYOUS » !

1992 Tim MAY, un grand scientifique travaillant chez Intel, lance la *mailing list* cryptée « Cypherpunk ».

Cypherpunk
8.5.12.12.15*

* HELLO !

1993 Eric HUGHES écrit un livre intitulé...

LE MANIFESTE D'UN CYPHERPUNK

C'est la première fois que le mot « cypherpunk » apparaît publiquement.

De nombreux sujets y sont abordés par les utilisateurs.

CRYPTOGRAPHIE

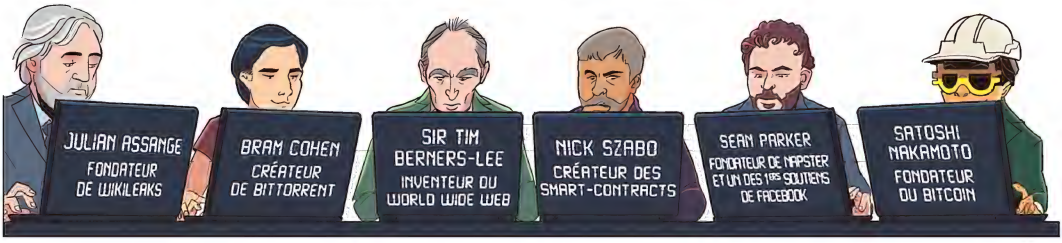
POLITIQUE

CYPHERPUNK 1400 UTILISATEURS

PHILOSOPHIE

PROBLÉMATIQUES PERSONNELLES

Les membres d'origine du réseau Cypherpunk sont des célébrités de l'industrie des technologies de l'information, comme...



AVANT LA NAISSANCE DU BITCOIN, LA COMMUNAUTÉ CYPHERPUNK AVAIT DÉJÀ INVENTÉ PLUS DE DIX SYSTÈMES DIFFÉRENTS DE MONNAIES NUMÉRIQUES ET DE SYSTÈMES DE PAIEMENT...

B-MONEY
BIT GOLD
HASHCASH
...

... MAIS AUCUN N'AVAIT VRAIMENT PERCÉ.

Et c'est là, avec ce fameux Bitcoin, que commence véritablement

L'AVENTURE DE LA BLOCKCHAIN.

LA NAISSANCE DU PREMIER BITCOIN !

Trois mois après la publication du *Livre blanc du Bitcoin*, le grand jour arriva...

OUiiii !

2009 3 JANVIER

Dans un petit serveur situé à Helsinki, en Finlande...

MON TOUT PREMIER BLOC BITCOIN, MINÉ DE MES PROPRES MAINS...

SNIF ! QUE DE FIERTÉ !

FÉLICITATIONS, MONSIEUR NAKAMOTO ! C'EST UN BEAU BLOC GENÈSE.

PAPA !

Ainsi, Satoshi NAKAMOTO reçut du système...

TROP CONTENT !

LES 50 PREMIERS JETONS BITCOIN !

POUR VOUS RÉCOMPENSER DE CET HEUREUX ÉVÉNEMENT.

LE BITCOIN (BTC) ÉTAIT NÉ !

Pour commémorer cette naissance du Bitcoin, Satoshi NAKAMOTO inséra dans le code de ce premier bloc un article du *Times* daté du même jour.

THE TIMES
3 JANVIER 2009
Opérations de sauvetage des banques britannique

BLOC GENÈSE

QUELLE BRILLANTE IDÉE D'AVOIR EU LA PRÉSENCE D'ESPRIT DE PRENDRE DATE ET D'AUTHENTIFIER LA NAISSANCE DU BITCOIN GRÂCE À CET ARTICLE !

L'IRONIE DANS TOUT ÇA, C'EST QUE LE SUJET TRAITÉ CE JOUR-LÀ CONCERNAIT LES OPÉRATIONS DE SAUVETAGE DES BANQUES BRITANNIQUES.

COMMENT LES BITCOINS SONT-ILS ÉMIS ?

Tout d'abord, QU'EST-CE QUE LE BITCOIN ?

LE SYSTÈME QUI PERMET D'ÉMETTRE CES BITCOINS EST ÉQUIVALENT À UN GRAND REGISTRE.

Il n'a pas d'émetteur spécifique et repose seulement sur un système de distribution décentralisé.

La tenue de ce registre est réalisée par des informaticiens appelés des « mineurs ».

Toutes les dix minutes, les mineurs se font concurrence pour être les premiers à trouver la solution à un problème mathématique complexe leur permettant d'obtenir le droit d'enregistrer sur ce grand registre une nouvelle page appelée « bloc ».

Pour chaque bloc enregistré, le mineur obtient une certaine quantité de bitcoins en récompense. Ces jetons bitcoin sont émis progressivement par le système.

C'est donc ainsi que ce processus de « minage » permet l'émission de nouveaux bitcoins.

COMMENT BITCOIN CONTRÔLE-T-IL SON OFFRE ?

Le Bitcoin est une monnaie virtuelle qui a été mise en place avec une offre limitée.

Le nombre total de bitcoins émis n'excédera pas...

21 MILLIONS DE JETONS

Lors de la conception du Bitcoin, NAKAMOTO définit pour chaque jeton bitcoin une limite de divisibilité à 1 centième de millionnième.

TOUT COMME 1 EURO PEUT ÊTRE DIVISÉ EN 100 CENTIMES D'EURO, LE BITCOIN PEUT ÊTRE DIVISÉ EN UNITÉS PLUS PETITES APPELÉES SATOSHIS.

100 000 000 SATOSHIS POUR ÊTRE PRÉCIS.

0,00000001
1 unité = 1 satoshi

En pratique, cette divisibilité permet en cas de hausse du bitcoin de le rendre accessible à tous et utilisable comme monnaie quotidienne.

VOUS POUVEZ MÊME ACHETER UN ORDINATEUR DE *GAMING* ALIENWARE EN UTILISANT DES BITCOINS !

PAF! PIF!

MAIS POURQUOI CETTE OFFRE PRÉPROGRAMMÉE ?

Cette limite fut fixée par Satoshi NAKAMOTO selon **DEUX RÈGLES** ...

Règle n° 1 :

1 bloc = 10 min.

210 000 blocs = 4 ans

Règle n° 2 : La récompense en bitcoins pour le minage d'un bloc est divisée successivement par 2 tous les 210 000 blocs.

JACKPOT !

50 JETONS

2009
0 à 210 000 blocs

?! GRAT GRAT

25 JETONS

2012
211 000 à 420 000 blocs

GLOUPS !

12,5 JETONS

2016
421 000 à 630 000 blocs

ARGH !

6,5 JETONS

14 MAI 2020
631 000 à 840 000 blocs

Vers l'an **2045**, **99,95 %** des bitcoins seront émis

LE TOUT DERNIER JETON. SNIF !

2140
20 790 000 à 21 000 000 blocs

Cette offre préprogrammée du Bitcoin provoqua tout un débat parmi les économistes.

CE SYSTÈME APPORTE UNE SOLIDITÉ INTRINSÈQUE !

MAIS POURQUOI EN LIMITER LA QUANTITÉ ?!

ON IMITE AINSI LES RÉSERVES D'OR !

BLA BLA BLA BLA BLA BLA BLA BLA BLA BLA

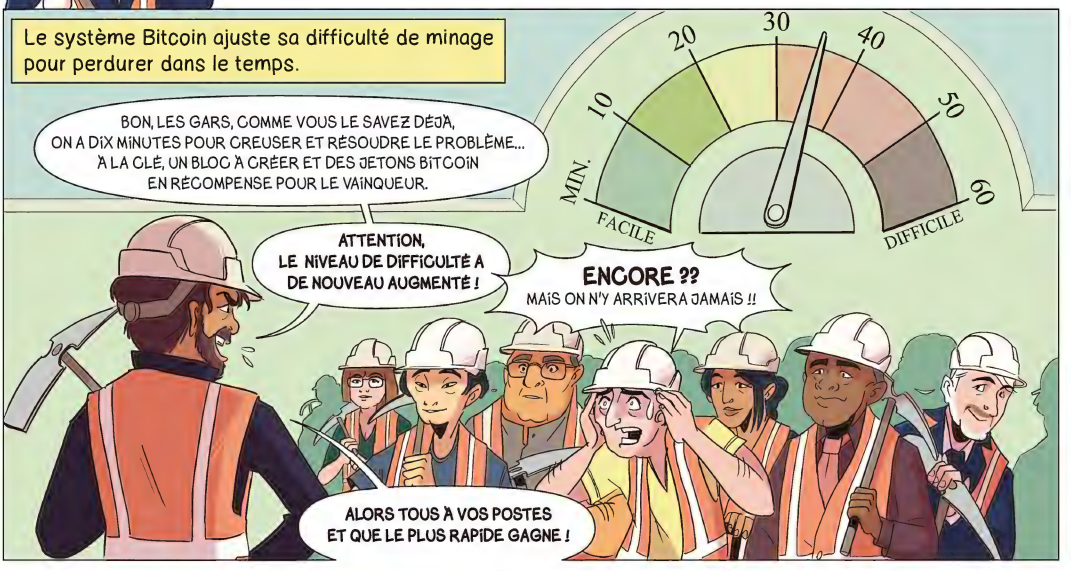
Ce mécanisme eut pour effet d'encourager les mineurs à commencer au plus vite leur activité.

... ET QUI DIT PLUS DE MINEURS, DIT PLUS DE PUISSANCE DE TRAITEMENT DES TRANSACTIONS...

... MAIS AUSSI PLUS DE SÉCURITÉ AU RÉSEAU, CAR CHAQUE MINEUR POSSÈDE UNE COPIE DU REGISTRE BITCOIN, OÙ LES BLOCS SONT RELIÉS ENTRE EUX.

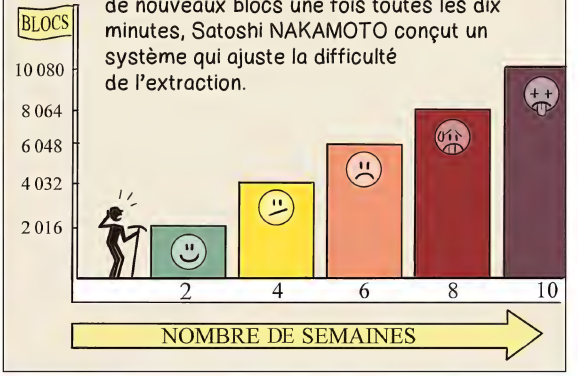
POURQUOI EST-IL ENCORE POSSIBLE DE MINER DES BITCOINS ?

Le système Bitcoin ajuste sa difficulté de minage pour perdurer dans le temps.

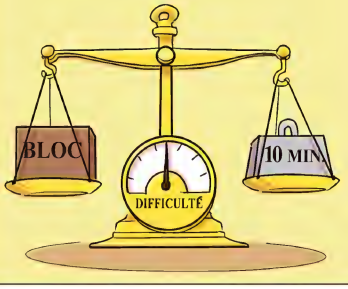


Imaginez si la puissance de calcul du réseau Bitcoin ne cessait d'augmenter....

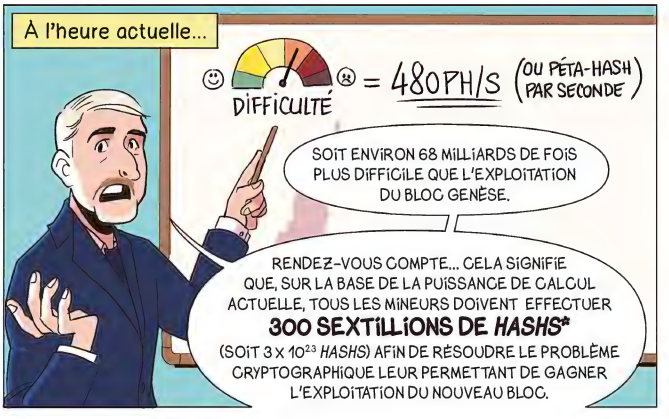
Pour justement maintenir le rythme de création de nouveaux blocs une fois toutes les dix minutes, Satoshi NAKAMOTO conçut un système qui ajuste la difficulté de l'extraction.



Ainsi, cette difficulté ajustée permet de maintenir le rythme de génération des nouveaux blocs à un seul bloc toutes les dix minutes.

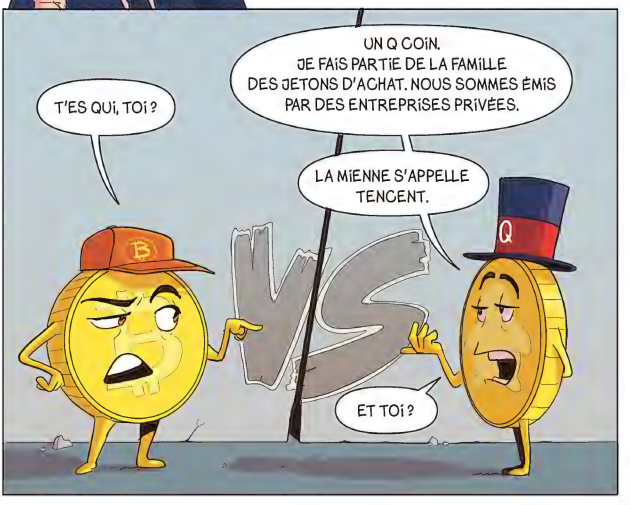


À l'heure actuelle...



* *Hash* = algorithme ou série d'opérations mathématiques effectuées par un ordinateur.

EN QUOI BITCOIN EST-IL DIFFÉRENT DES JETONS D'ACHAT COMME LES Q COINS ?



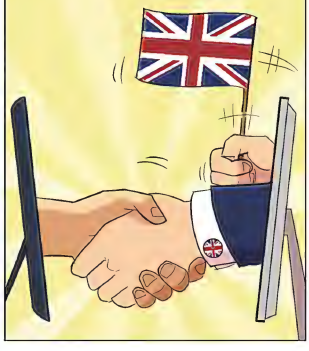
DEUX PIZZAS À PLUS DE 100 MILLIONS DE DOLLARS !

Le 22 mai 2010

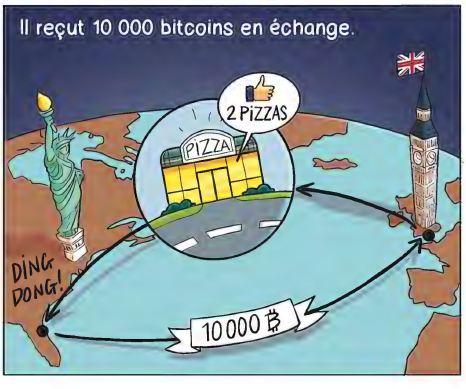
Laszlo HANYECZ, un programmeur américain et fan de Bitcoin, essaya d'utiliser des jetons bitcoin pour échanger des biens.

Il posta une annonce sur un forum Bitcoin...

Un volontaire britannique conclut la transaction avec HANYECZ.



Il reçut 10 000 bitcoins en échange.



C'était la première fois qu'un prix était associé à des jetons bitcoin, ce qui suscita un vif émoi au sein de la communauté crypto.

D'ailleurs, pour commémorer cette toute première transaction, le 22 mai est devenu la journée « BITCOIN PIZZA », où les amateurs de Bitcoin de tous les pays se rassemblent pour la célébrer en mangeant une pizza.

Rendez-vous compte, selon le cours du bitcoin, ces deux pizzas valaient dix ans plus tard...

Laszlo HANYECZ est sûrement inconsolable du montant de cette première transaction !

LE SUCCESSEUR DE NAKAMOTO, GAVIN ANDRESEN

Gavin ANDRESEN est l'un des principaux membres de l'équipe de développement du Bitcoin.

... ET L'UN DES RARES À AVOIR ÉCHANGÉ PAR E-MAIL AVEC SATOSHI NAKAMOTO AVANT QU'IL NE DISPARAÎSSE.

Dès 2010, Gavin s'intéressa au Bitcoin.

Il commença à proposer des algorithmes à NAKAMOTO.

TRÈS INTÉRESSANT !

Monsieur Nakamoto,

Voici quelques algorithmes pour optimiser le système de base du Bitcoin.

Gavin Andresen

Et NAKAMOTO commença progressivement à faire confiance au code de Gavin.

Un jour...

Cher Gavin,

Accepteriez-vous d'inscrire votre adresse e-mail sur la page d'accueil de Bitcoin ?

Satoshi Nakamoto

C'est ainsi qu'en 2011, Satoshi NAKAMOTO se retira en coulisses.

Désormais chef de file de la communauté Bitcoin, Gavin forma l'équipe de développement principale du système Bitcoin.

MES CHERS CAMARADES, VOTRE MISSION, SI VOUS L'ACCEPTEZ, SERA DE CORRIGER LES FAILLES DU CODE DE BITCOIN ET D'AMÉLIORER LA STABILITÉ DU LOGICIEL.

En 2012, Gavin créa la BITCOIN FOUNDATION, une organisation à but non lucratif.

CLAP! CLAP! CLAP!

LE SUCCÈS DE BITCOIN EST PRINCIPALEMENT DÛ AUX CONTRIBUTIONS REMARQUABLES DE GAVIN ANDRESEN ET DE SON ÉQUIPE.

LE « ROBINET AUX BITCOINS »

Au cours des premières années de la création du système Bitcoin, les jetons étaient bon marché et très faciles à acquérir.

Par exemple, fin 2010...

De plus, Gavin ANDRESEN créa un site web appelé...

Ce « robinet aux bitcoins » faisait sa publicité en distribuant des bitcoins.

Cette démarche publicitaire connut un très grand succès.

Plus tard, des émules imitèrent Gavin en construisant des sites similaires, qui donnaient une petite quantité de bitcoins à leurs visiteurs.

Ces sites générèrent un trafic important.

Ils purent ainsi récolter des frais de publicité de la part de plateformes d'échange qui souhaitaient y faire leur promotion.

ENVIRON 50 % DES PLATEFORMES D'ÉCHANGE DE BITCOINS DÉPENDAIENT ALORS DE CES PUBLICITÉS POUR LEUR TRAFIC, CE QUI EN FIT À L'ÉPOQUE UN MODÈLE ÉCONOMIQUE TRÈS VIABLE.

C'est ainsi que le système Bitcoin commença à se faire connaître du grand public, et qu'il grandit progressivement en notoriété.

QUELLES POLITIQUES GOUVERNEMENTALES ENVERS LES CRYPTOS ?

À l'échelle mondiale, tous les pays n'ont pas la même politique à l'égard de la *blockchain* et des crypto-monnaies.

D'ailleurs, de manière générale, les États sont encore dans une phase d'apprentissage.

Peu à peu, les pays imposent des réglementations aux crypto-actifs.

ÉTATS-UNIS

Le Bitcoin est considéré comme une *commodity*, ou matière première.

Par exemple, à New York...

NOUS ÉMETTONS DES LICENCES COMMERCIALES D'ACTIVITÉ DE MONNAIE VIRTUELLE, APPELÉES BITLICENSES.

LA PREMIÈRE A ÉTÉ DÉLIVRÉE EN 2015 ET, CINQ ANS PLUS TARD, ON EN COMPTE 25 OFFICIELLEMENT APPROUVÉES.

ALLEMAGNE

NOUS SOMMES LE PREMIER PAYS À RECONNAÎTRE LES CRYPTO-MONNAIES EN TANT QUE « MONNAIES PRIVÉES ».

JAPON

Très favorable aux crypto-monnaies, le pays adopte une loi dès avril 2017.

NOUS ACCEPTONS OFFICIELLEMENT LE BITCOIN COMME MÉTHODE DE PAIEMENT LÉGALE !

CORÉE DU SUD

Une réglementation plus stricte est préconisée.

En juillet 2017, le pays adopte un projet de loi réglementaire.

DORÉNAVANT, TOUS LES CRYPTO-INVESTISSEURS DEVRONT DISPOSER D'UN CAPITAL MINIMAL DE 500 MILLIONS DE WON.

CHINE

En octobre 2021, le pays interdit officiellement le Bitcoin.

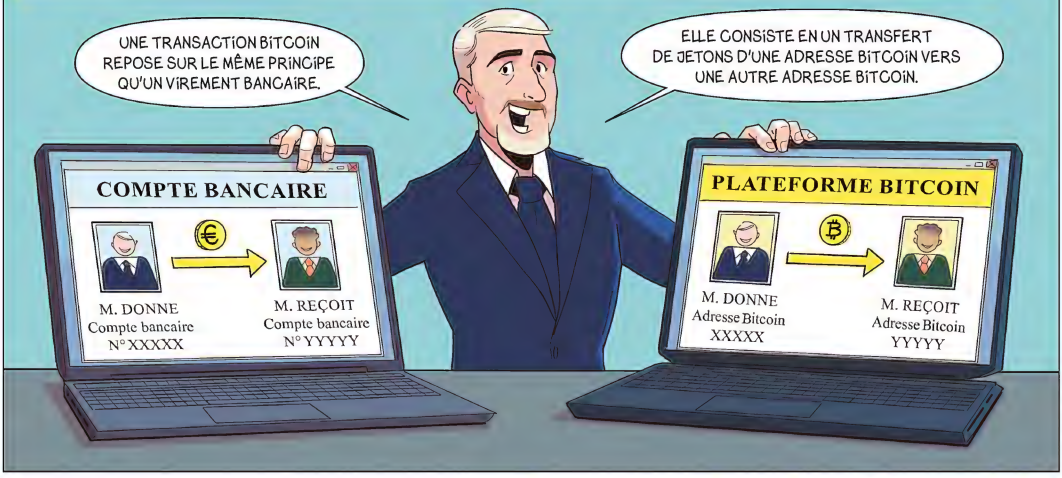
DORÉNAVANT, LE MINAGE ET LES TRANSACTIONS EN CRYPTO-MONNAIES SONT INTERDITS SUR NOTRE TERRITOIRE.

CHAPITRE 2

LE BITCOIN EN PRATIQUE

COMMENT FONCTIONNENT LES TRANSACTIONS EN BITCOINS ?

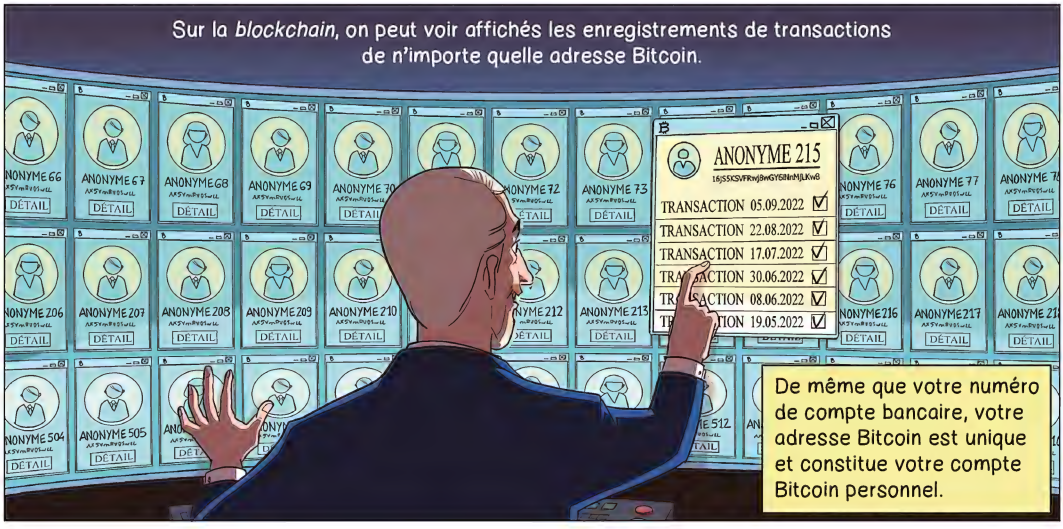
Nous avons tous un compte bancaire individuel qui, par son système dématérialisé, facilite le transfert d'argent notamment entre particuliers.

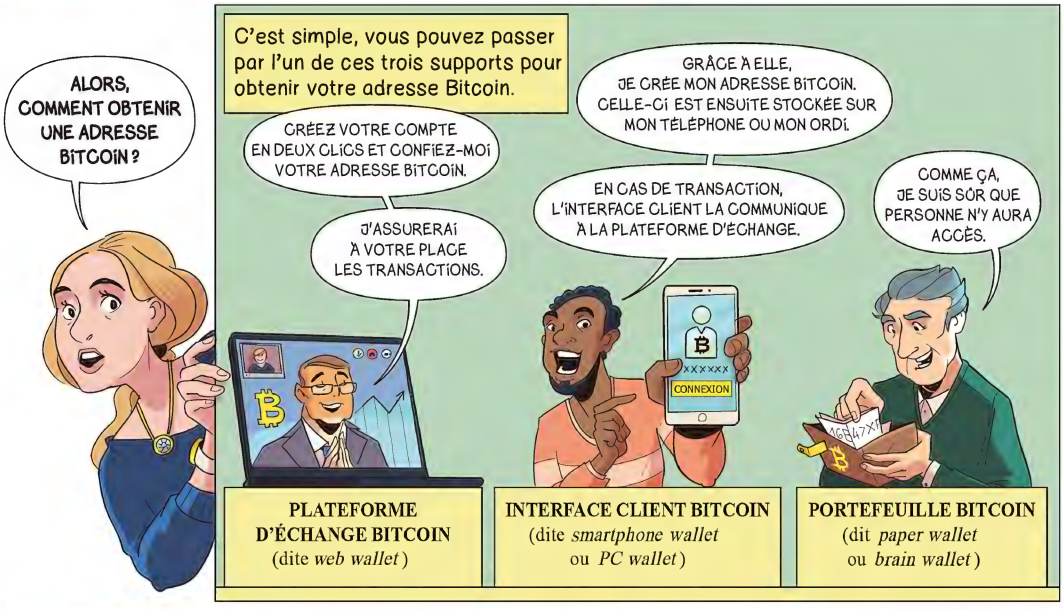


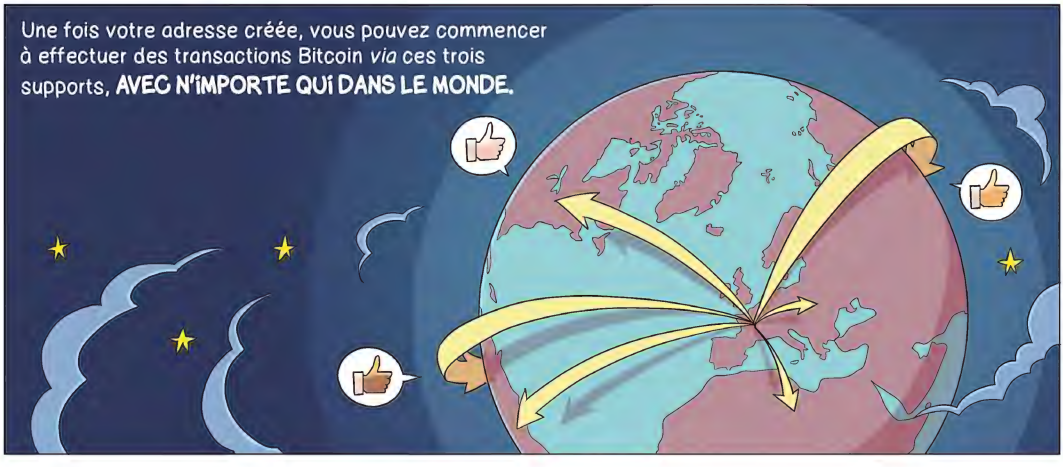
Si vous souhaitez envoyer des jetons à quelqu'un, il vous suffit de renseigner...

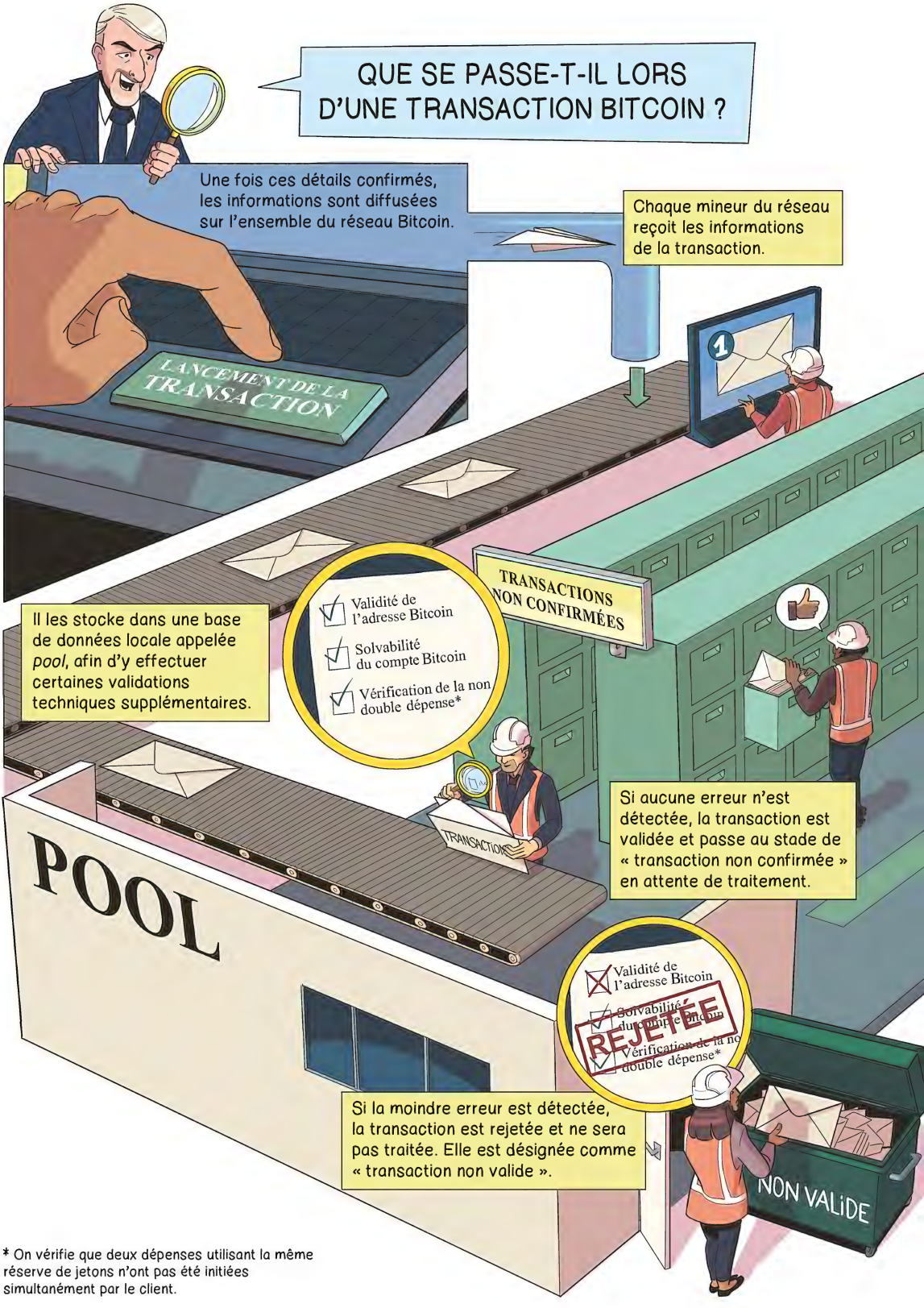
Une adresse Bitcoin est composée de 26 à 35 caractères alphanumériques aléatoires.

16jS5KSVFRwj8wGY6iNnMjLKw8


Sur la *blockchain*, on peut voir affichés les enregistrements de transactions de n'importe quelle adresse Bitcoin.
ANONYME 215
TRANSACTION 05.09.2022
TRANSACTION 22.08.2022
TRANSACTION 17.07.2022
TRANSACTION 30.06.2022
TRANSACTION 08.06.2022
TRANSACTION 19.05.2022
De même que votre numéro de compte bancaire, votre adresse Bitcoin est unique et constitue votre compte Bitcoin personnel.

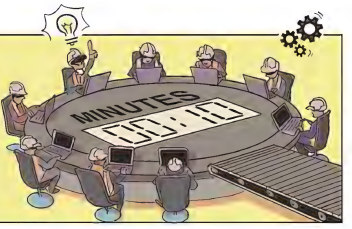

ALORS, COMMENT OBTENIR UNE ADRESSE BITCOIN ?
C'est simple, vous pouvez passer par l'un de ces trois supports pour obtenir votre adresse Bitcoin.
CRÉEZ VOTRE COMPTE EN DEUX CLICS ET CONFIEZ-MOI VOTRE ADRESSE BITCOIN.
J'ASSURERAI À VOTRE PLACE LES TRANSACTIONS.
GRÂCE À ELLE, JE CRÉE MON ADRESSE BITCOIN. CELLE-CI EST ENSUITE STOCKÉE SUR MON TÉLÉPHONE OU MON ORDI.
EN CAS DE TRANSACTION, L'INTERFACE CLIENT LA COMMUNIQUE À LA PLATEFORME D'ÉCHANGE.
COMME ÇA, JE SUIS SÛR QUE PERSONNE N'Y AURA ACCÈS.
CONNEXION
PLATEFORME D'ÉCHANGE BITCOIN (dite *web wallet*)
INTERFACE CLIENT BITCOIN (dite *smartphone wallet* ou *PC wallet*)
PORTEFEUILLE BITCOIN (dit *paper wallet* ou *brain wallet*)


Une fois votre adresse créée, vous pouvez commencer à effectuer des transactions Bitcoin *via* ces trois supports, **AVEC N'IMPORTE QUI DANS LE MONDE.**



* On vérifie que deux dépenses utilisant la même réserve de jetons n'ont pas été initiées simultanément par le client.

Les mineurs se font concurrence pour traiter et mettre à jour cette liste de « transactions non confirmées » en tentant d'être le premier à achever le calcul cryptographique (ou hachage) permettant leur enregistrement.



BLOCKCHAIN

Le premier à réussir cette étape gagne le droit de mettre à jour le grand registre.

Il se saisit alors d'environ 1 000 transactions stockées dans son *pool* de « transactions non confirmées » et les dépose dans un nouveau bloc.

BLOC

BLOC

BLO

Une fois le bloc chaîné aux autres dans la chaîne de blocs, plus de possibilité de contestation ou d'altération du registre. Les transactions sont inscrites de manière définitive dans la *blockchain* Bitcoin.

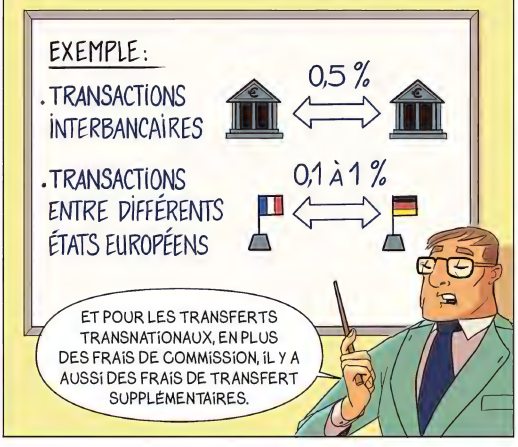
CES 1 000 TRANSACTIONS EN ATTENTE SONT DÉPOSÉES DANS UN NOUVEAU BLOC TOUTES LES DIX MINUTES.

CELLES QUI N'ONT PU ÊTRE TRAITÉES À TEMPS, EN RAISON DE LEUR NOMBRE TROP ÉLEVÉ, DEVRONT ATTENDRE LA CRÉATION D'UN NOUVEAU BLOC.

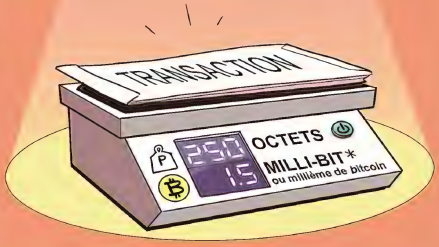
Une fois ces étapes passées, vos jetons bitcoin sont désormais disponibles dans le portefeuille du destinataire.

QUELS FRAIS POUR LES TRANSACTIONS BITCOIN ?

Les banques facturent généralement des frais représentant un pourcentage du montant de la transaction.



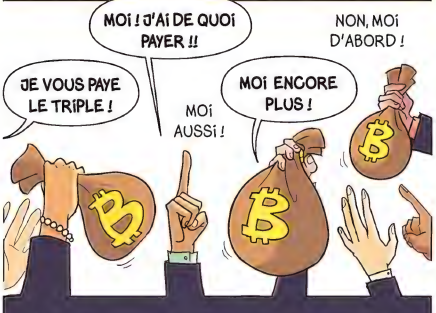
Pour les crypto-monnaies, les frais de transaction sont basés sur la taille de la transaction en octets, et non sur le montant transféré.



* Environ 1 à 1,5 millième de bitcoin.

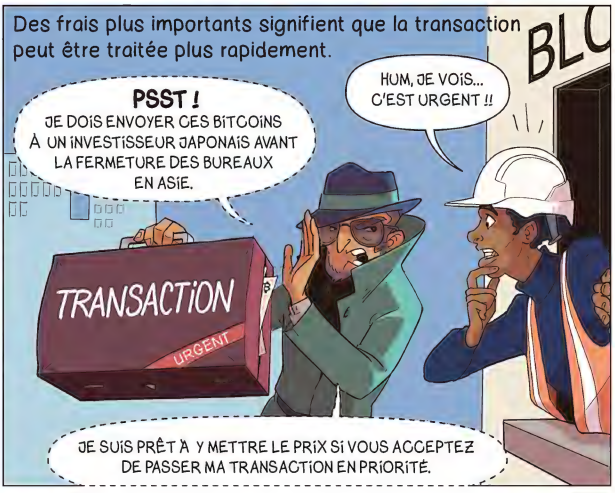
Les blocs-registres étant de taille limitée, ils ne peuvent contenir qu'un nombre limité de transactions...

Par conséquent, les mineurs priorisent les transactions qui offrent les frais les plus élevés.

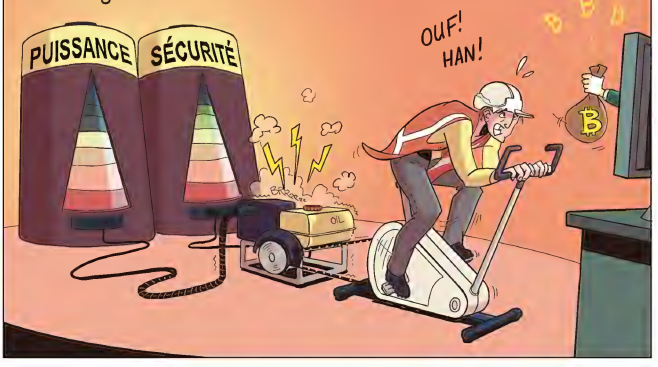


Il revient à l'émetteur de la transaction de décider du montant de ces frais.

Des frais plus importants signifient que la transaction peut être traitée plus rapidement.



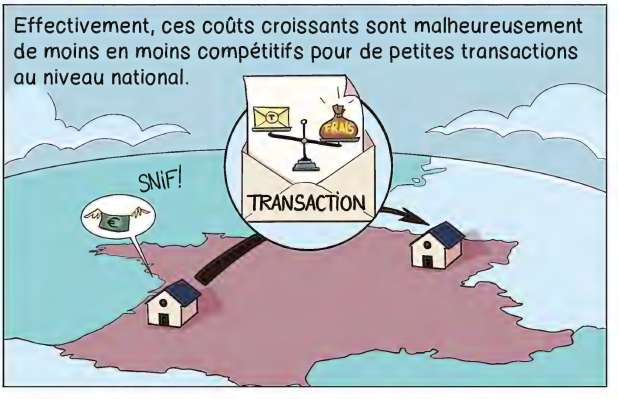
Ainsi, ces frais de transaction Bitcoin ont pour but d'inciter les mineurs à fournir une puissance de hachage suffisante...



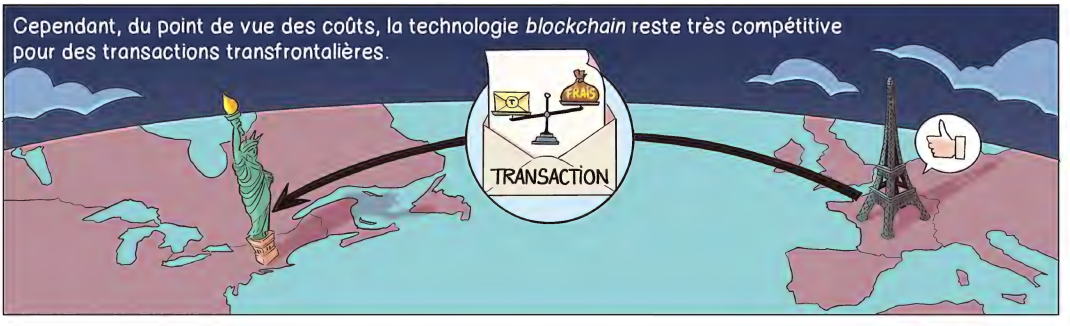
... mais également à maintenir le réseau Bitcoin même après l'extraction de tous les jetons bitcoin !

Et qui dit plus de puissance de hachage, dit plus de sécurité sur le réseau, protégeant ainsi efficacement la *blockchain* des spams.

Effectivement, ces coûts croissants sont malheureusement de moins en moins compétitifs pour de petites transactions au niveau national.



Cependant, du point de vue des coûts, la technologie *blockchain* reste très compétitive pour des transactions transfrontalières.



QU'EST-CE QU'UN NŒUD BITCOIN ?

Bitcoin étant un système de paiement électronique de particulier à particulier, chaque portefeuille agit comme un nœud de transmission.

Ainsi, pour chaque transaction, l'expéditeur envoie des informations aux nœuds environnants...

... qui diffusent cette information à d'autres nœuds environnants...

... couvrant ainsi l'ensemble du réseau.

ON DISTINGUE DEUX TYPES DE NŒUDS.

Les nœuds dit « SIMPLES » sont uniquement des relais d'information.

Les nœuds dit « COMPLETS » sont des points névralgiques du réseau. En plus de gérer la diffusion et la validation des transactions, ils stockent la totalité des informations de la *blockchain*.

Ainsi, après validation de la transaction, ce sont les nœuds complets qui inscrivent la transaction sur la *blockchain*.

EN OCTOBRE 2017, LE RÉSEAU BITCOIN COMPTAIT 9 300 NŒUDS COMPLETS EN ACTIVITÉ. EN 2022, ON EN COMPTE ENVIRON 10 000.

Les États-Unis, l'Allemagne et la France ont le plus grand nombre de nœuds complets Bitcoin.

Quant à la Chine, elle représentait encore 5 % des nœuds complets dans le monde jusqu'à l'interdiction d'octobre 2021.

PUISQU'IL N'Y A AUCUNE RÉCOMPENSE SPÉCIFIQUE POUR LA MAINTENANCE DES NŒUDS ET QUE LES BITCOINS PEUVENT TOUJOURS ÊTRE TRANSFÉRÉS SANS AVOIR BESOIN DE CES NŒUDS COMPLETS, ILS PEUVENT RESTER EN QUANTITÉ LIMITÉE ET NE REPRÉSENTER QU'UN FAIBLE POURCENTAGE DE L'ENSEMBLE DES NŒUDS DANS LE RÉSEAU...

... QUI, QUANT À EUX, NE CESSENT DE CROÎTRE.

0

NŒUDS SIMPLES

NŒUDS COMPLETS

LA SIGNATURE NUMÉRIQUE BITCOIN

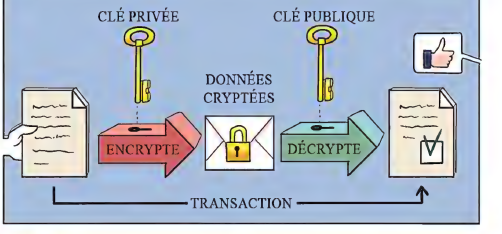
Une des forces du système Bitcoin est sa capacité à garantir la sécurité des transactions et de son contenu dans l'univers peu sécurisé qu'est celui d'Internet.

La signature numérique est une des clés de ce système hyper-sécurisé.

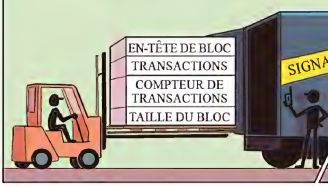
La signature numérique se compose d'une série de codes inviolables.

Au contraire, cette série de codes cache un cryptage très complexe qui utilise des algorithmes de chiffrement Digital Digest et des techniques dites de « cryptographie asymétrique ».

La cryptographie asymétrique fait référence à l'utilisation d'une clé privée pour le chiffrement et d'une clé publique pour le déchiffrement.

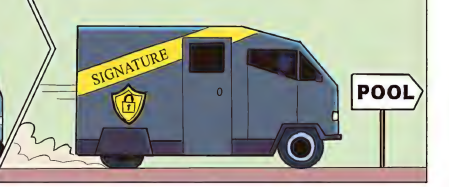


En pratique, le chiffrement Digital Digest compresse les informations...

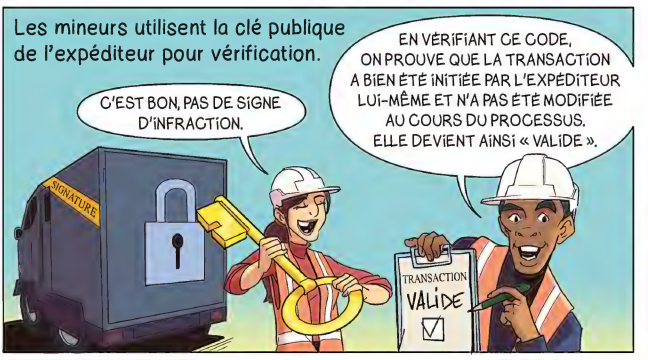


... puis utilise la clé privée pour les crypter en une signature numérique.

Une fois terminé, ce cryptage regroupe le message de la transaction avec la signature et les envoie aux mineurs.



Les mineurs utilisent la clé publique de l'expéditeur pour vérification.

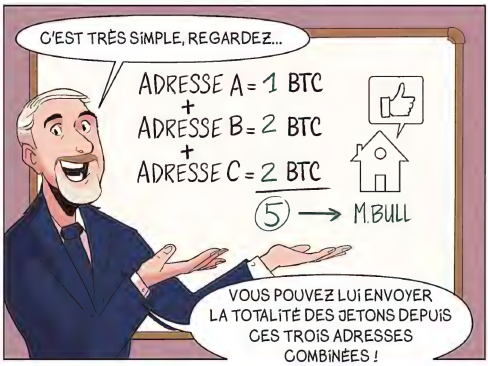


Tout comme un code de carte bancaire, elle est propre à chaque utilisateur et doit rester secrète.

QUELQUES PRÉCISIONS SUR L'ENVOI DE BITCOINS

Au même titre qu'une personne peut posséder plusieurs comptes bancaires à son nom, il est possible de posséder plusieurs adresses Bitcoin.

CAS N° 1 : ENVOI DE BITCOINS À PARTIR DE PLUSIEURS ADRESSES



CAS N° 2 : ENVOI DE BITCOINS À PLUSIEURS ADRESSES EN UNE SEULE TRANSACTION

CHAPITRE 3

LE PROCESSUS DE MINAGE

LE MINAGE EN PRATIQUE

Le Bitcoin adopte un « système mis à jour distribué* » qui oblige le mineur à se battre pour être le premier à créer un nouveau bloc.

5... 4... 3...

??

SORS, T'AS PLUS LE TEMPS !!

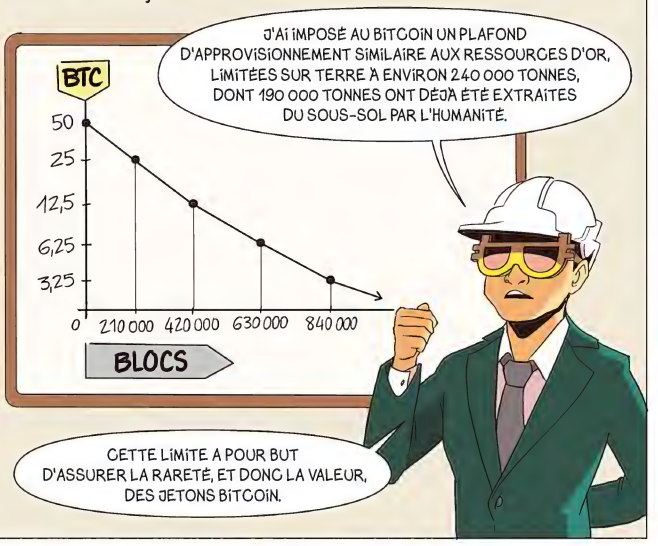
CAFÉ

* Ou *distributed updated system* en anglais.

En récompense, le vainqueur reçoit des jetons.

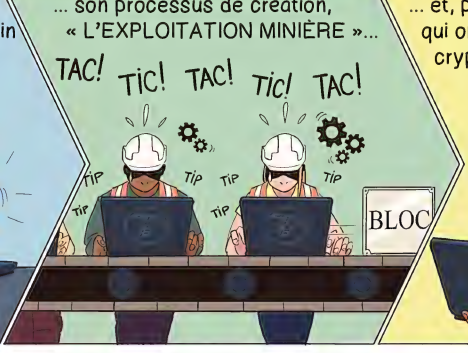
C'est grâce à ce processus de minage que ces derniers sont produits.

Satoshi NAKAMOTO a conçu le système de telle sorte que cette récompense soit divisée par 2 tous les 210 000 blocs jusqu'à atteindre la limite de divisibilité fixée à 1 centième de millionième de jeton.



Du fait de cette analogie, on appelle souvent le Bitcoin « L'OR NUMÉRIQUE »...

... son processus de création, « L'EXPLOITATION MINIÈRE »...

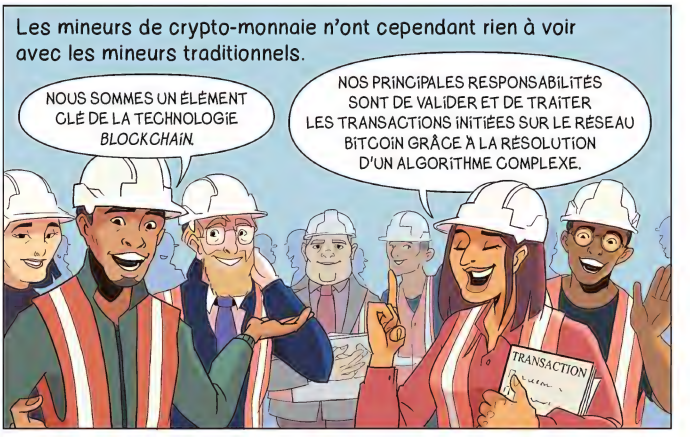


... et, par extension, les personnes qui opèrent le « minage » des crypto-monnaies « LES MINEURS ».

QUI SONT LES MINEURS ?

Vous avez sûrement en tête l'image d'un homme éprouvé par un travail pénible dans les mines de charbon, avec le corps recouvert de suie ?

Les mineurs de crypto-monnaie n'ont cependant rien à voir avec les mineurs traditionnels.



Je vous expliquerai très prochainement ce que sont une ferme de minage et un *pool* de minage.

QU'EST-CE QU'UNE *MINING RIG* ?

Les *mining rigs* sont des plateformes de minage.

LES PLATEFORMES SONT L'ÉQUIVALENT DU « CERVEAU » DU PROCESSEUR CENTRAL D'UN PC.

ELLES RÉSOLVENT DES PROBLÈMES MATHÉMATIQUES COMPLEXES PERMETTANT L'ENREGISTREMENT DES TRANSACTIONS DANS LA *BLOCKCHAIN* BITCOIN.

Elles sont commercialisées sous forme d'un assemblage de...

VENTILATEURS

PUCE ASICs

CIRCUITS INTÉGRÉS SPÉCIALISÉS (OU ASICs) DÉDIÉS AU MINAGE

Ils constituent le composant central d'une *mining rig*.

BOÎTIER DE SUPPORT DES CIRCUITS INTÉGRÉS

ALIMENTATION

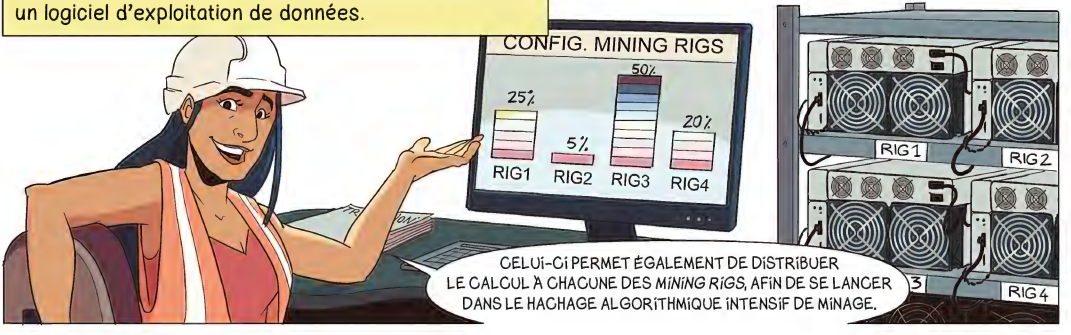
DISSIPATEURS THERMIQUES

VENTILATEURS

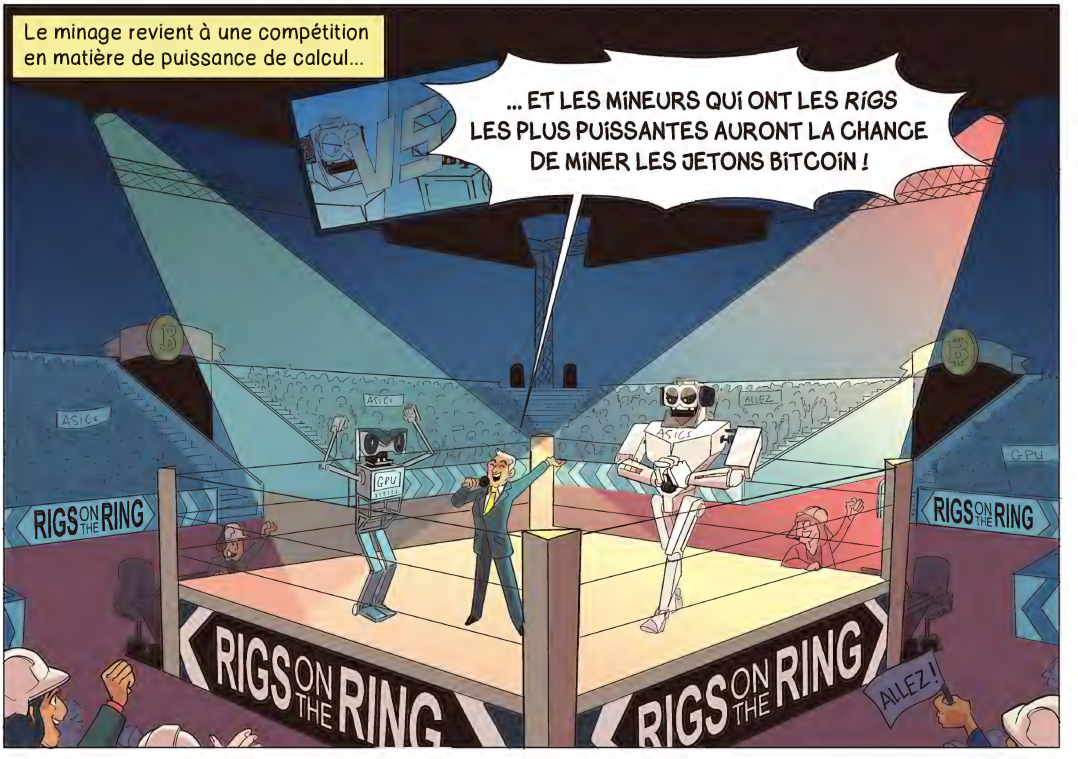
LES *MINING RIGS* CONSOMMENT EN EFFET BEAUCOUP D'ÉNERGIE.

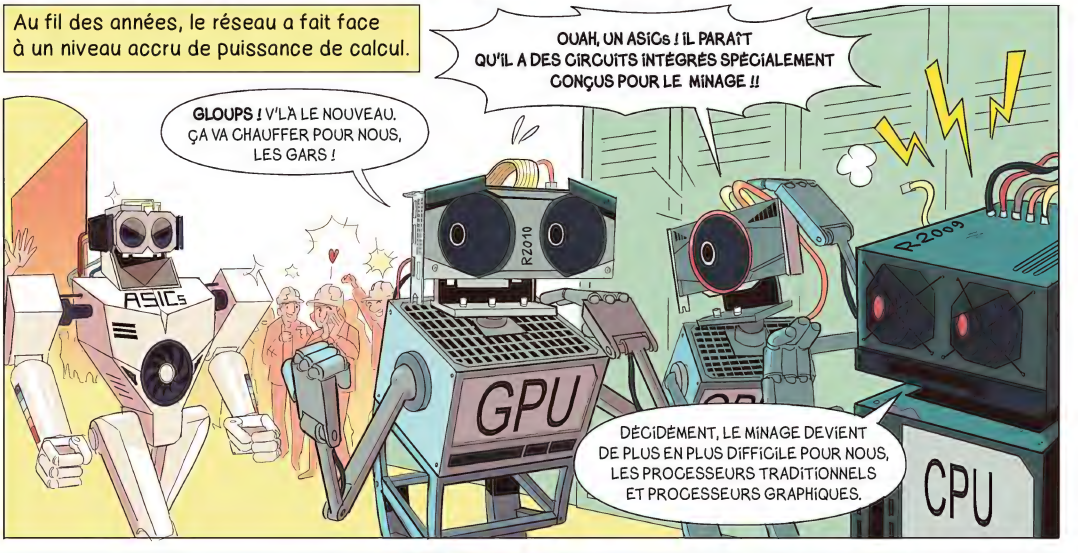
Ces plateformes peuvent surchauffer pendant le processus. C'est pourquoi des dissipateurs de chaleur et des ventilateurs sont installés à des fins de refroidissement.

Pour contrôler les *mining rigs*, les mineurs téléchargent un logiciel d'exploitation de données.



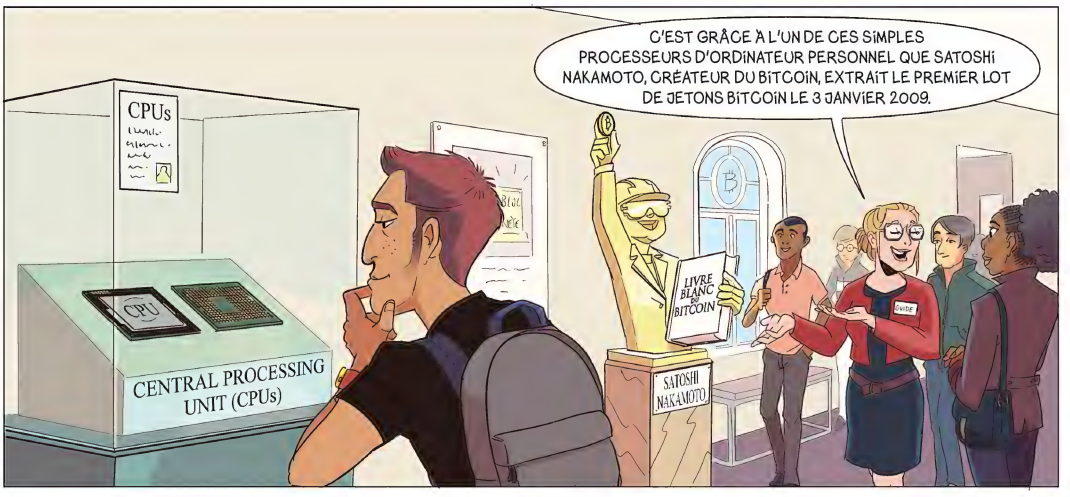
CELUI-CI PERMET ÉGALEMENT DE DISTRIBUER LE CALCUL À CHACUNE DES *MINING RIGS*, AFIN DE SE LANCER DANS LE HACHAGE ALGORITHMIQUE INTENSIF DE MINAGE.


Le minage revient à une compétition en matière de puissance de calcul...
... ET LES MINEURS QUI ONT LES *RIGS* LES PLUS PUISSANTES AURONT LA CHANCE DE MINER LES JETONS BITCOIN !
RIGS ON THE RING
RIGS ON THE RING
RIGS ON THE RING
ALLEZ !
ASICs
GPU
ALLEZ
G-PU


Au fil des années, le réseau a fait face à un niveau accru de puissance de calcul.
OUAH, UN ASICs ! IL PARAÎT QU'IL A DES CIRCUITS INTÉGRÉS SPÉCIALEMENT CONÇUS POUR LE MINAGE !!
GLOUPS ! V'LÀ LE NOUVEAU. ÇA VA CHAUFFER POUR NOUS, LES GARS !
ASICs
R2010
R-2009
GPU
DÉCIDÉMENT, LE MINAGE DEVIENT DE PLUS EN PLUS DIFFICILE POUR NOUS, LES PROCESSEURS TRADITIONNELS ET PROCESSEURS GRAPHIQUES.
CPU

L'ALGORITHME DE MINAGE POUR CHAQUE CRYPTO-MONNAIE EST DIFFÉRENT.
IL EXISTE DONC DES *RIGS* DIFFÉRENTES, AVEC DES CIRCUITS INTÉGRÉS DÉDIÉS SPÉCIFIQUEMENT À CHAQUE CRYPTO-MONNAIE.
MINING MARKET
▷ RIGS BITCOIN
▷ RIGS ETHEREUM
▷ RIGS LITECOIN
▷ RIGS DASH

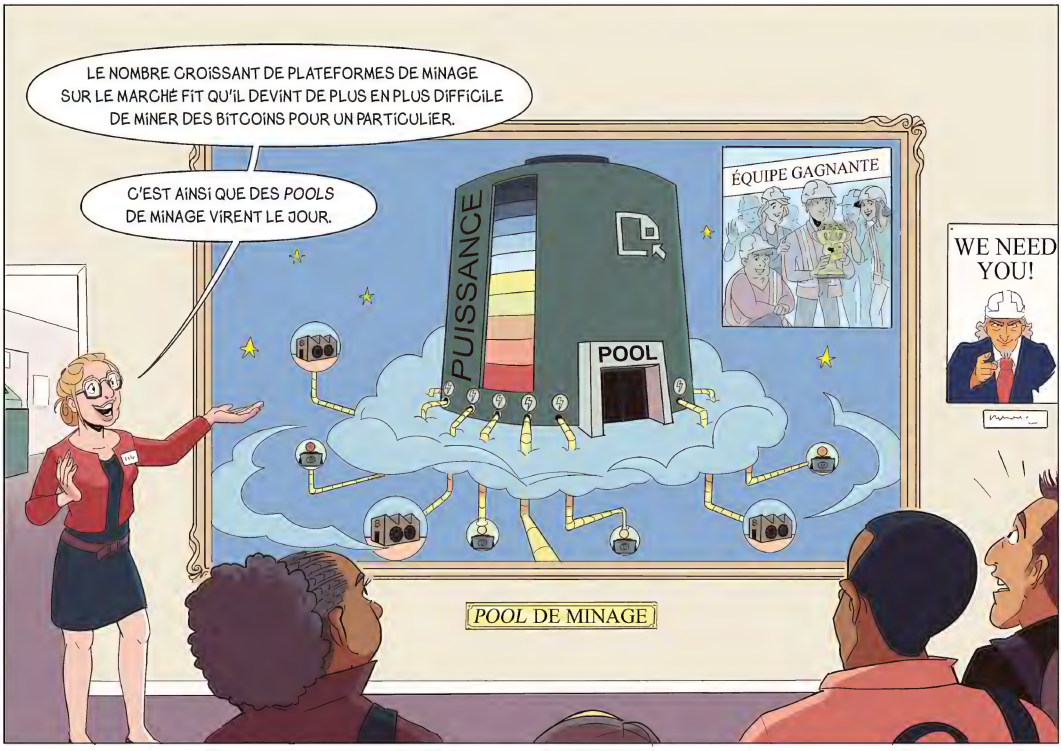
MINAGE AVEC DES PROCESSEURS TRADITIONNELS, OU CPUs



MINAGE AVEC DES PROCESSEURS GRAPHIQUES, OU GPUs

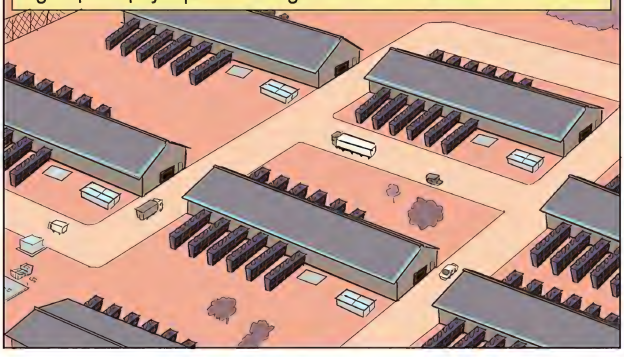
UTILISATION DE *RIGS*, OU PLATEFORMES

REGROUPEMENT COLLECTIF EN *POOLS* DE MINAGE



À QUOI RESSEMBLE UNE FERME DE MINAGE ?

Les fermes de minage sont des lieux où les *rigs* de minage sont regroupées physiquement et gérées de manière centralisée.



Elles sont généralement situées dans des pays, et plus spécifiquement dans des zones géographiques, où l'électricité est relativement bon marché et où sa production est stable.

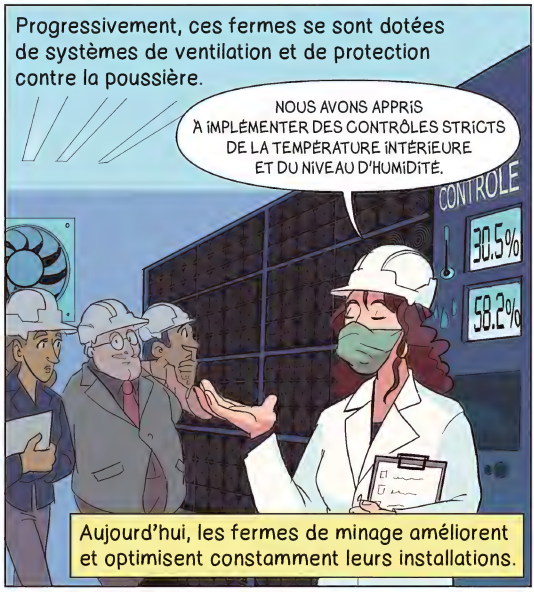
1	ETATS-UNIS	35%
2	KAZAKHSTAN	18%
3	RUSSIE	11%
4	CANADA	10%
5	IRLANDE	5%
6	MALAISIE	5%
7	ALLEMAGNE	4%

Classement janvier 2022.

Au début, les fermes de minage ne faisaient pas l'objet d'une maintenance très sérieuse.

Elles consistaient simplement en des étagères où s'empilaient les *rigs* de minage.

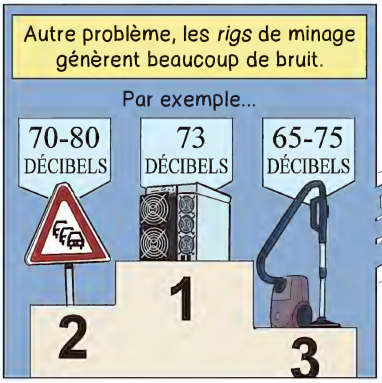
Progressivement, ces fermes se sont dotées de systèmes de ventilation et de protection contre la poussière.



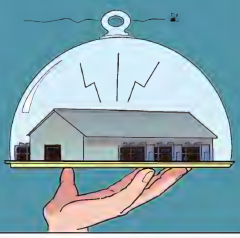
Aujourd'hui, les fermes de minage améliorent et optimisent constamment leurs installations.

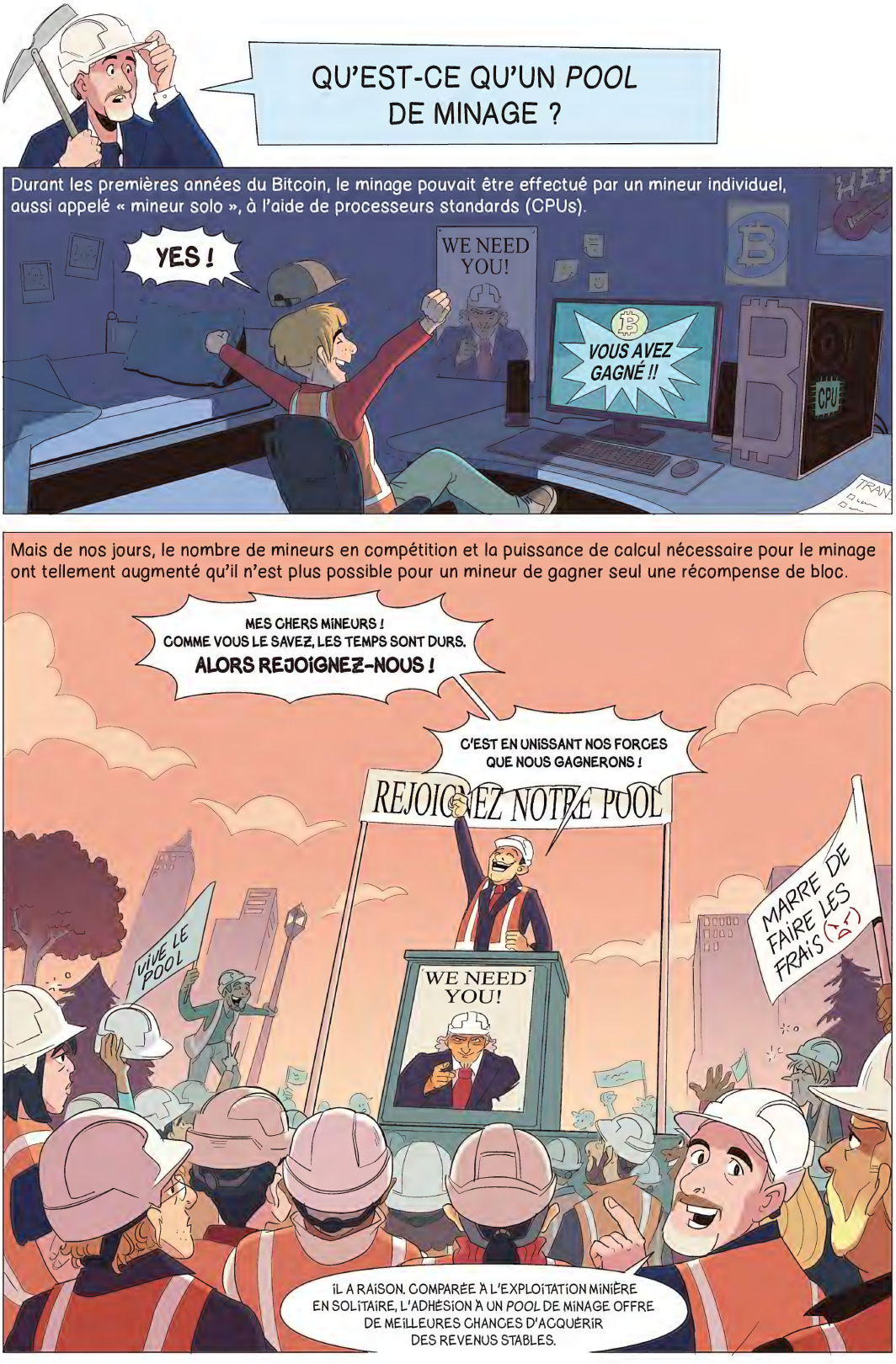
Peu à peu, les mineurs prirent conscience que ces plateformes se détérioraient rapidement.

Autre problème, les *rigs* de minage génèrent beaucoup de bruit.



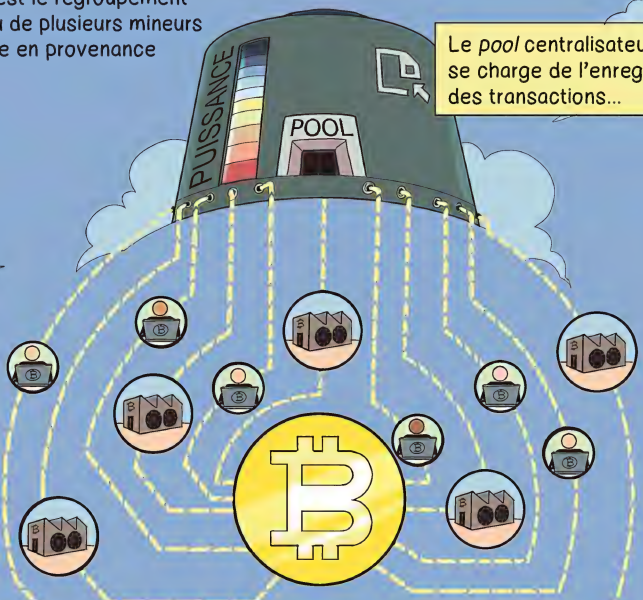
Par conséquent, des fermes insonorisées ont vu le jour, intégrant de nombreuses modifications et améliorations.




QU'EST-CE QU'UN *POOL* DE MINAGE ?
Durant les premières années du Bitcoin, le minage pouvait être effectué par un mineur individuel, aussi appelé « mineur solo », à l'aide de processeurs standards (CPUs).
YES !
WE NEED YOU!
VOUS AVEZ GAGNÉ !!
CPU
Mais de nos jours, le nombre de mineurs en compétition et la puissance de calcul nécessaire pour le minage ont tellement augmenté qu'il n'est plus possible pour un mineur de gagner seul une récompense de bloc.
MES CHERS MINEURS !
COMME VOUS LE SAVEZ, LES TEMPS SONT DURS.
ALORS REJOIGNEZ-NOUS !
C'EST EN UNISSANT NOS FORCES QUE NOUS GAGNERONS !
REJOIGNEZ NOTRE POOL
VIVE LE POOL
WE NEED YOU!
MARRE DE FAIRE LES FRAIS
IL A RAISON. COMPARÉE À L'EXPLOITATION MINIÈRE EN SOLITAIRE, L'ADHÉSION À UN *POOL* DE MINAGE OFFRE DE MEILLEURES CHANCES D'ACQUÉRIR DES REVENUS STABLES.

Un *pool* de minage est le regroupement sur un même réseau de plusieurs mineurs et fermes de minage en provenance du monde entier...

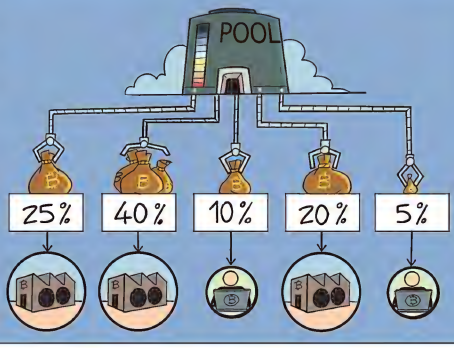
Le *pool* centralisateur se charge de l'enregistrement des transactions...

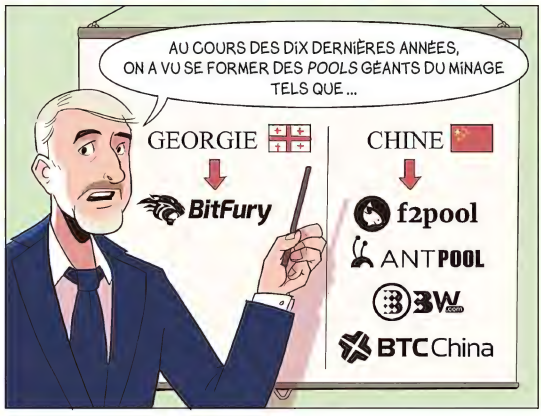


... tandis que les mineurs individuels ou fermes de minage qui lui sont associés combinent leurs ressources afin de lui fournir la puissance de calcul nécessaire au processus compétitif.

Grâce à cette puissance de calcul agrégée, le *pool* de minage a plus de chances de peser significativement dans la course à l'obtention du droit d'inscription sur le grand registre de la *blockchain*.

Le *pool* redistribue ensuite la récompense de bloc à ses adhérents, au prorata de leurs contributions.





QU'EST-CE QUE LA CAPACITÉ DE HACHAGE ?

Au cours du processus de minage, les mineurs doivent résoudre des problèmes mathématiques complexes.

CEPENDANT, LA SOLUTION NE PEUT PAS ÊTRE TROUVÉE EN UTILISANT UNE FORMULE DÉFINIE.

ÇA SERAIT TROP FACILE SINON !

Les mineurs font donc appel à un nombre gigantesque d'essais pour trouver la bonne solution.

138E ESSAI... J'ESPÈRE QUE CETTE FOIS, C'EST LE BON !

NOUVEL ESSAI

Celle-ci a pour nom...

CORRECT HASH

LE NOMBRE D'ESSAIS QU'UNE PLATEFORME MINIÈRE PEUT EFFECTUER PAR SECONDE REPRÉSENTE SA PUISSANCE DE CALCUL, AUSSI APPELÉE « CAPACITÉ DE HACHAGE ».

ELLE EST MESURÉE EN HASH PAR SECONDE.

À l'heure actuelle, les plateformes minières traditionnelles sont livrées avec une puissance de calcul de 50 Térahash par seconde, voire 100 Th/s pour les meilleures.

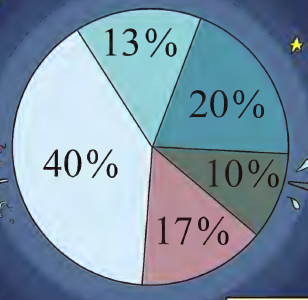
100 000 Mds DE CALCULS PAR SECONDE

Elles sont appelées MINEURS 50T OU 100T en référence à leur puissance.

La puissance de hachage d'un mineur par rapport à la puissance de calcul de l'ensemble du réseau correspond au pourcentage de chances qu'il a de gagner la récompense de bloc toutes les dix minutes.

Ainsi, si la puissance de calcul du réseau Bitcoin est à 100...

YES, ENCORE GAGNÉ !



C'EST TROP DUR ! J'AI SEULEMENT 10 % DE CHANCES DE GAGNER LA RÉCOMPENSE DE BLOC !!

Autrement dit, la capacité de hachage mesure la puissance de traitement du réseau.

QU'EST-CE QUE LA COMPTABILITÉ CONCURRENTIELLE ?

La comptabilité concurrentielle* désigne la méthode utilisée par le réseau Bitcoin pour assurer l'enregistrement des transactions.

J'ASSURE ET MAINTIENS L'INTÉGRITÉ ET LA COHÉRENCE DE CE GRAND REGISTRE DE COMPTES PARTAGÉ.

REGISTRE

COPIE

* Ou *competitive book-keeping* en anglais.

Le système Bitcoin ne dépend pas d'une autorité centrale pour assurer sa comptabilité.

Chaque nœud a le droit de participer à cet exercice.

... ASSURER LA COHÉRENCE DU REGISTRE EST LA PRIORITÉ DU SYSTÈME, ET DONC DE CHACUN DE NOUS !

Dans le réseau Bitcoin, chaque mineur entre en compétition pour gagner un droit d'écriture sur le registre comptable...

QUI VEUT GAGNER DES BITCOINS ?

TOP, À VOS CLAVIERS !

VOUS AVEZ DIX MINUTES POUR RÉSOUDRE LE PROBLÈME MATHÉMATIQUE COMPLEXE POSÉ.

... ET CEUX QUI ONT UNE CAPACITÉ DE HACHAGE PLUS ÉLEVÉE ONT PLUS DE CHANCES DE GAGNER CETTE COMPÉTITION.

SUPER CALCULATOR

REGISTRE

METTRE À JOUR

START

EN TANT QUE VAINQUEUR, À VOUS L'HONNEUR DE METTRE À JOUR **LE GRAND REGISTRE.**

Il en partage ensuite la dernière version à l'ensemble du réseau.

REGISTRE COPIE

En retour, il reçoit en récompense de nouveaux jetons bitcoin générés par le système en cette occasion.

QUI VEUT GAGNER DES BITCOINS ?

CANDIDATURES

LORSQUE LE PRIX DU BITCOIN AUGMENTE, DE NOMBREUX MINEURS SONT ATTIRÉS POUR TENTER DE GAGNER CE DROIT DE MISE À JOUR DU REGISTRE.

CANDIDATURE

STAFF

LE RÉSEAU DOIT AJUSTER À LA HAUSSE LA DIFFICULTÉ DU PROCHAIN EXERCICE DE MINAGE.

CHAPITRE 4

LE BITÇOIN COMME VÉHICULE D'INVESTISSEMENT

QUELS OUTILS POUR INVESTIR DANS LES CRYPTO-ACTIFS ?

Depuis 2008 et la parution du *Livre blanc du Bitcoin*, de nouveaux types de crypto-monnaies sont apparus...

... faisant naturellement évoluer les méthodes pour investir dans cette nouvelle classe d'actifs.

À l'origine, les utilisateurs de Bitcoin étaient principalement des geeks.

Au fil des années, de plus en plus de professionnels s'y sont intéressés.

Désormais, de nombreux produits financiers sont disponibles pour capitaliser sur ces crypto-monnaies.

Il existe aussi différents types de plateformes, parmi lesquelles...

PLATEFORMES D'ÉCHANGE EN LIGNE

PROCÉDURES DE TRANSACTIONS DE GRÉ À GRÉ
ou OTC (*over the counter*)

PLATEFORMES DE TRADING CENTRALISÉES ET DÉCENTRALISÉES

COMMENT UTILISER UNE PLATEFORME D'ÉCHANGE ?

L'achat direct de crypto-monnaies sur des plateformes d'échange est de loin le moyen le plus simple pour investir.

SUPER ! J'AI LE CHOIX ENTRE PLEIN DE PLATEFORMES : BINANCE, COINBASE, HUOBI, BITFINEX OU KRAKEN.

ALLEZ, JE ME LANCE !

TRADING CRYPTO-MONNAIES

START

Ces plateformes ont le même principe de fonctionnement que les Bourses des marchés d'actions.

Elles collectent les ordres d'achat et de vente...

... puis les comparent, de manière anonyme.

Elles les regroupent ensuite par paires, toujours de manière anonyme, de sorte que l'on ne connaît pas la contrepartie à qui l'on a vendu ou acheté.

Enfin, elles enregistrent et publient tous les ordres, qu'il s'agisse d'un ordre d'achat ou de vente.

VENTE

ACHAT

VENTE

PLATEFORME

CETTE CONTREPARTIE PEUT D'AILLEURS ÊTRE UNE PERSONNE UNIQUE, OU UN GROUPE DE PERSONNES.

TRANSACTIONS

$ 12 678

$ 12 892

VENTE

VENTE

ACHAT

x2

Expéditeur : ANONYME

x2

Expéditeur : ANONYME

x2

De surcroît, la Bourse collecte les prix et le volume des transactions pour convertir ces données sous forme de graphiques dits « en chandeliers japonais ».

CHAQUE « BOUGIE » REPRÉSENTE NON SEULEMENT LES COURS DU DÉBUT ET DE FIN DE SÉANCE, MAIS AUSSI LES NIVEAUX MAXIMUM ET MINIMUM ATTEINTS EN COURS DE SÉANCE.

PRIX

"BAR CHART" VOLUME

Ces représentations sont utilisées par les analystes « chartistes ».

NOUS TENTONS D'ANALYSER GRAPHIQUEMENT LA TENDANCE DU MARCHÉ, EN ESPÉRANT Y TROUVER DES MOTIFS RÉCURRENTS.

COMMENT FONCTIONNE LE TRADING DE GRÉ À GRÉ ?

Ce type de transaction, également appelé OTC, permet à des acheteurs et des vendeurs de coter des prix et d'échanger entre eux des denrées ou des biens, sans la supervision d'une Bourse.

Depuis toujours, les êtres humains utilisent l'échange de gré à gré pour leurs opérations de trading, allant des céréales aux marchés aux poissons.

Sur le marché, les acheteurs et les vendeurs se font face, en direct. Sans intermédiaire, l'échange est efficace.

Mais il peut s'avérer parfois risqué, car il faut faire confiance au vendeur, s'assurer de la qualité du bien qu'il vend...

Dans le cadre d'un échange de gré à gré, les deux parties peuvent négocier le prix avant de conclure la transaction, soit en face-à-face, soit par téléphone ou tout autre moyen de communication.

Par opposition, les marchés organisés, aussi appelés Bourses ou plateformes d'échange, offrent aux vendeurs et aux acheteurs une structure pour faciliter leurs échanges.

Ces plateformes n'apparurent que bien plus tard, comme la Bourse du riz de Dojima, à Osaka, qui ne vit le jour qu'en 1697.

Les échanges se font par l'intermédiaire de courtiers.

La Bourse protège l'acheteur contre un risque de défaut du vendeur, et elle assure la qualité des biens qui y sont vendus.

Il y a même des employés de la Bourse qui policent ces échanges.

Lors de l'apparition de Bitcoin, il n'existait pas de plateforme d'échange.

Les investisseurs ont donc commencé par traiter de gré à gré...

... ET J'EXIGE UN PAIEMENT COMPTANT.

MAIS DÉSORMAIS, IL EXISTE DE NOMBREUSES PLATEFORMES FACILITANT LES ÉCHANGES OTC STANDARDISÉS. REGARDE !

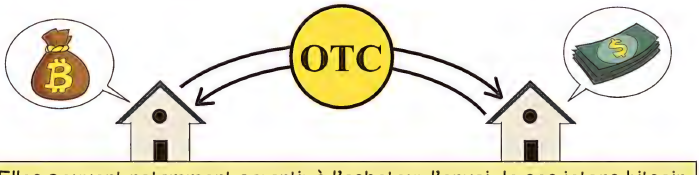
PRINCIPAUX FACILITATEURS DE TRADING OTC

- LocalBitcoins
- Genesis Trading
- Coinbase Prime
- B2C2
- HiveEx
- Kraken OTC
- Huobi OTC
- Binance OTC

GRÂCE À ELLES, LES ACHETEURS ET LES VENDEURS PEUVENT CHOISIR DIRECTEMENT AVEC QUI ILS SOUHAITENT NÉGOCIER.

OUI, MAIS QUELLES GARANTIES OFFRENT CES PLATEFORMES ?

En plus d'offrir une simplicité similaire à celle des Bourses d'échange, ces plateformes de trading OTC de renom proposent également certaines garanties de mitigation de risque.



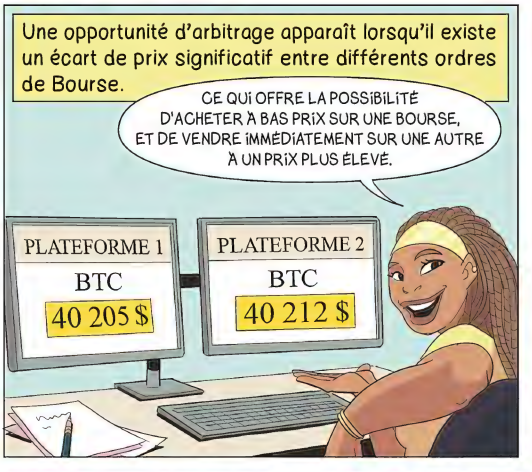
Elles peuvent notamment garantir à l'acheteur l'envoi de ses jetons bitcoin dès réception de son paiement.

QU'EST-CE QUE LE TRADING QUANTITATIF ?

Le trading quantitatif, ou trading algorithmique, utilise des ordres de trading préétablis, sur la base de modèles mathématiques.

Il existe différents types de trading quantitatif, tels que...

Une opportunité d'arbitrage apparaît lorsqu'il existe un écart de prix significatif entre différents ordres de Bourse.

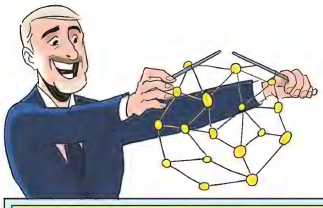


Le trading de tendance est plus complexe.

Et enfin, le trading de « couverture », ou *hedging trading*, est un type de prise de position inspiré des marchés des changes.

Il consiste à couvrir, totalement ou partiellement, le risque financier d'un investissement à l'aide d'un autre investissement.

L'émergence de ces différentes techniques de trading automatisé a fortement contribué à la maturité de ces marchés, leur apportant de la liquidité, mais aussi de la volatilité.



QU'EST-CE QU'UNE PLATEFORME D'ÉCHANGE DÉCENTRALISÉE ?

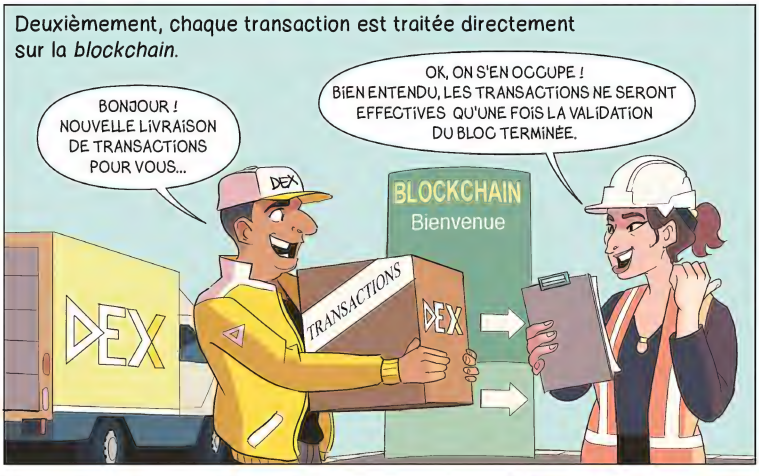
De nombreuses plateformes, aussi appelées DEX, pour *decentralized exchanges*, ont vu le jour dès 2013.

Parmi les plus connues, on peut citer...

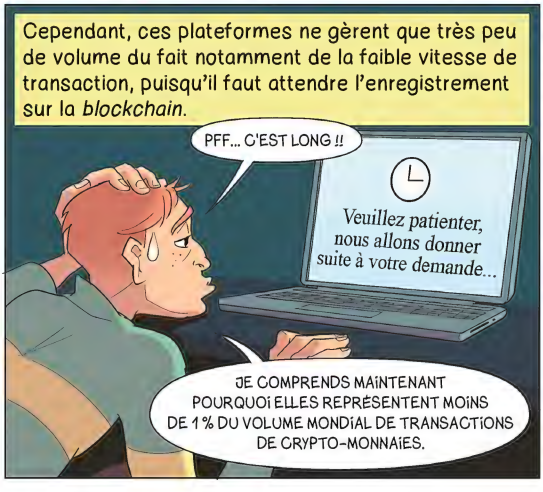
- AirSwap Protocol
- Kyber Protocol
- 0x Protocol
- OmiseGo
- Binance DEX

Premièrement, elles n'obligent pas les utilisateurs à divulguer leur identité.

Deuxièmement, chaque transaction est traitée directement sur la *blockchain*.



Cependant, ces plateformes ne gèrent que très peu de volume du fait notamment de la faible vitesse de transaction, puisqu'il faut attendre l'enregistrement sur la *blockchain*.



POURQUOI UTILISER UN PORTEFEUILLE BITCOIN ?

Le portefeuille Bitcoin stocke les informations de votre compte Bitcoin telles que...

ADRESSE BITCOIN
Équivaut au numéro de compte bancaire

CLÉ PRIVÉE
Équivaut au code secret de votre carte bancaire

DE MÊME QUE NOS PORTEFEUILLES PHYSIQUES PEUVENT CONTENIR PLUSIEURS CARTES BANCAIRES, UN PORTEFEUILLE BITCOIN PEUT AUSSI STOCKER PLUSIEURS ADRESSES BITCOIN...

ADRESSE 1
ADRESSE 2
ADRESSE 3

... AINSI QUE LA CLÉ PRIVÉE CORRESPONDANT À CHACUNE D'ENTRE ELLES.

Les portefeuilles Bitcoin se présentent sous de nombreuses formes, comme...

VOUS POUVEZ ÉGALEMENT ÉCRIRE VOTRE CLÉ PRIVÉE SUR UN SUPPORT PHYSIQUE TEL QUE CE CARNET...

... OU UTILISER CE QU'ON APPELLE UN *BRAIN WALLET* EN LA MÉMORISANT.

WWW

PORTEFEUILLES CLIENTS
Installés sur PC ou smartphone

PORTEFEUILLES WEB
Accessibles par Internet

PAPER WALLET

Leur fonction principale est de protéger votre clé privée.

MAIS ATTENTION, N'OUBLIEZ PAS QUE, CONTRAIREMENT À UN COMPTE BANCAIRE ADMINISTRÉ PAR UNE BANQUE, LE SYSTÈME BITCOIN NE REPOSE SUR AUCUNE AUTORITÉ CENTRALE.

OH NON !!
J'AI PERDU MON PORTEFEUILLE !

EN CAS DE PERTE OU DE VOL, VOUS NE POURREZ PAS FAIRE OPPOSITION ET VOS BITCOINS SERONT DÉFINITIVEMENT PERDUS.

La sécurité du stockage de vos données Bitcoin relève donc de votre seule responsabilité.

À VOUS DE CHOISIR LE TYPE DE PORTEFEUILLE DONT VOUS SAUREZ ASSURER LA MEILLEURE PROTECTION.

Ne mettez pas tous vos œufs dans le même panier, pensez à stocker vos informations à différents endroits pour réduire les risques !

COLD WALLET ET HOT WALLET

Vos portefeuilles Bitcoin peuvent être désignés comme *cold wallet* ou *hot wallet* en fonction de la manière dont vous décidez de stocker votre clé privée...

Les *cold wallets* sont stockés hors ligne.

Ils utilisent des appareils qui ne sont pas connectés à Internet pour assurer la sécurité de la clé privée.

Mais ils ne sont pas à l'abri d'autres risques, tels que le vol, la perte physique ou la casse.

Les *hot wallets*, à l'inverse, vous permettent d'accéder à votre clé privée directement en ligne.

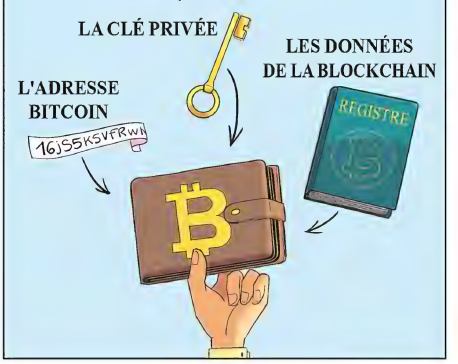
Aussi, si vous êtes tenté par la simplicité d'un *hot wallet*, il est préférable d'assurer la sécurité de vos crypto-monnaies en...

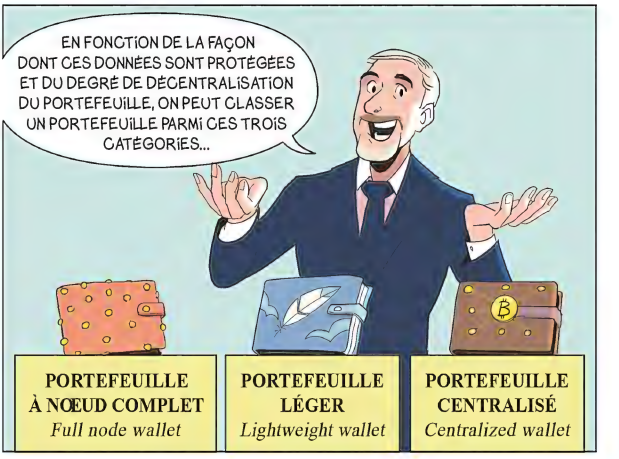
Attention cependant, car dans les deux cas, les gens peuvent voler vos bitcoins simplement en prenant connaissance de votre clé privée Bitcoin.

Aucun n'est absolument sans risque !

LES NŒUDS COMPLETS ET LES PORTEFEUILLES EN LIGNE

Nous avons déjà introduit différents types de portefeuilles ainsi que leur principal objectif qui est de stocker...

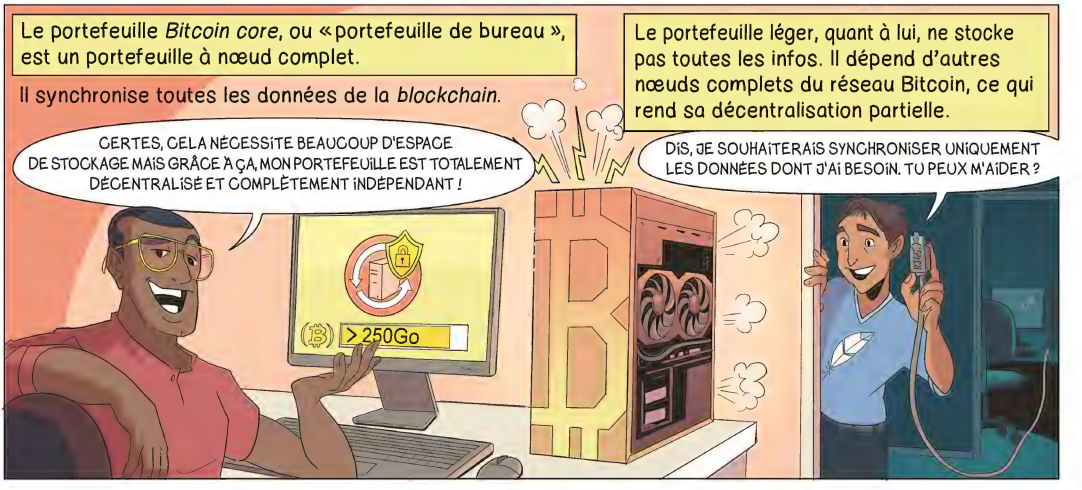




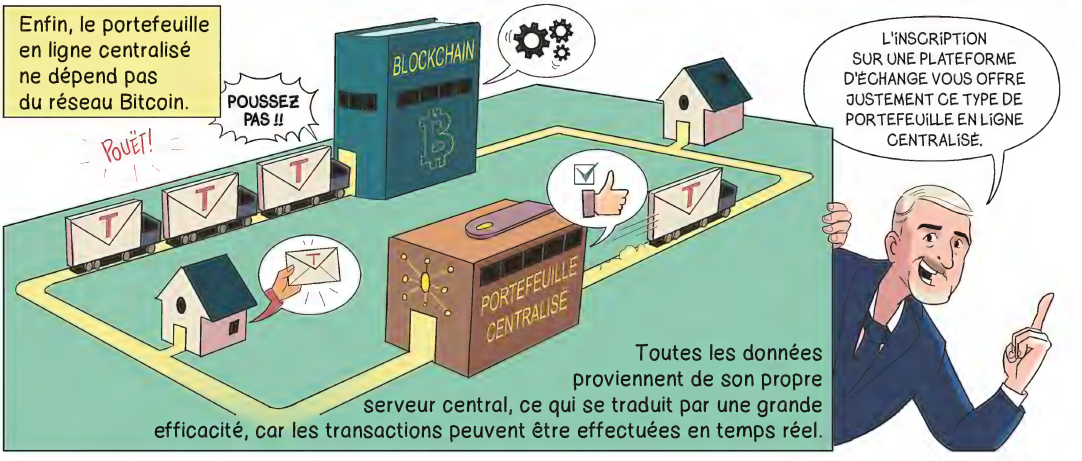
Le portefeuille *Bitcoin core*, ou « portefeuille de bureau », est un portefeuille à nœud complet.

Il synchronise toutes les données de la *blockchain*.

Le portefeuille léger, quant à lui, ne stocke pas toutes les infos. Il dépend d'autres nœuds complets du réseau Bitcoin, ce qui rend sa décentralisation partielle.



Enfin, le portefeuille en ligne centralisé ne dépend pas du réseau Bitcoin.



Toutes les données proviennent de son propre serveur central, ce qui se traduit par une grande efficacité, car les transactions peuvent être effectuées en temps réel.

PUIS-JE UTILISER DES JETONS BITCOIN COMME MOYEN DE PAIEMENT ?

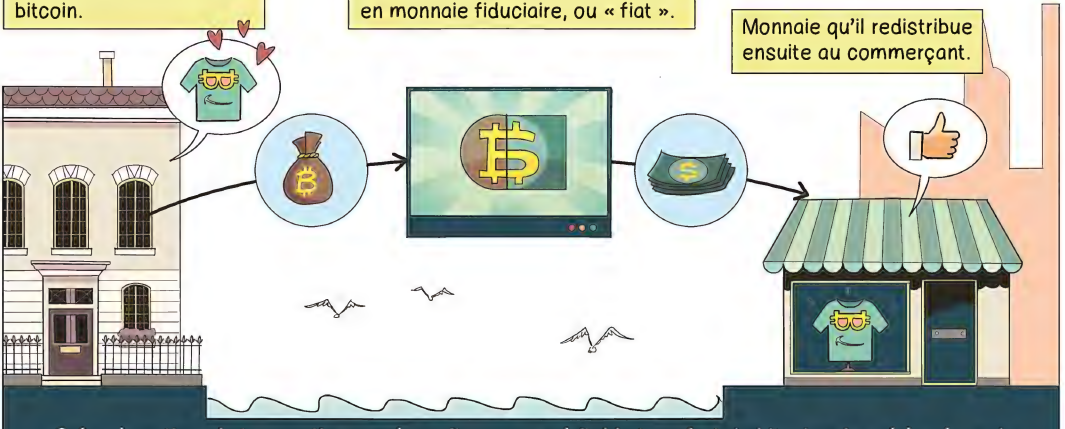
En tant que monnaie numérique, le Bitcoin est un mode de paiement accepté dans différents pays tels que...

La plupart des commerçants acceptent les jetons bitcoin par l'intermédiaire d'un processeur de paiement tiers.

Les clients paient d'abord en utilisant des jetons bitcoin.

Puis le processeur de paiement prend ces bitcoins et les convertit en monnaie fiduciaire, ou « fiat ».

Monnaie qu'il redistribue ensuite au commerçant.



Grâce à ce tiers, la transaction ne nécessite pas un véritable transfert de bitcoins de gré à gré, seuls les soldes actifs des deux parties sont modifiés, ce qui rend le paiement en bitcoins instantané.

Payer avec Bitcoin est facile !

La validation des deux parties est ensuite redemandée avant que le paiement soit effectué.

À la différence des outils de paiement en ligne comme ApplePay, lorsque vous utilisez des bitcoins pour le paiement, leur taux de change en temps réel apparaît après que vous avez scanné le QR code.

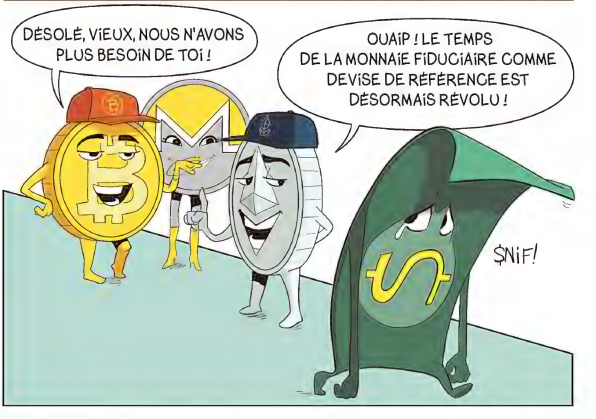
COMMENT ÉCHANGER DES CRYPTO-MONNAIES ENTRE ELLES ?

Avec le nombre croissant de crypto-monnaies, le dollar ne peut plus être une devise de référence auprès des investisseurs du monde entier.

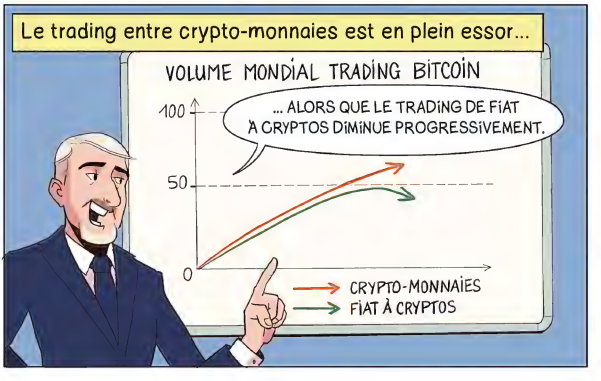
Ainsi, de plus en plus d'entre eux utilisent les plus reconnues, telles que le bitcoin, comme devise de référence pour coter la valeur d'autres crypto-monnaies.

Par exemple, le taux ETH/BTC utilise le bitcoin comme référence pour coter l'éthereum.

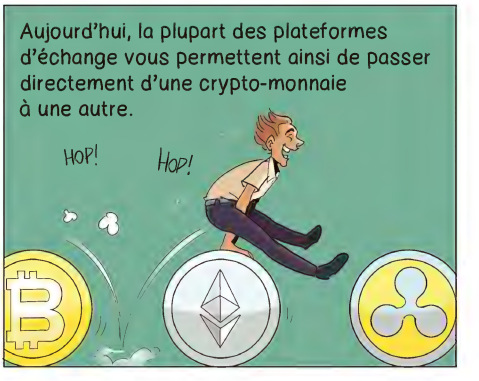
Grâce à ces taux de change basés sur la valeur de référence d'une crypto-monnaie, et non plus du dollar, vous pouvez échanger une crypto-monnaie contre une autre directement.



Le trading entre crypto-monnaies est en plein essor...

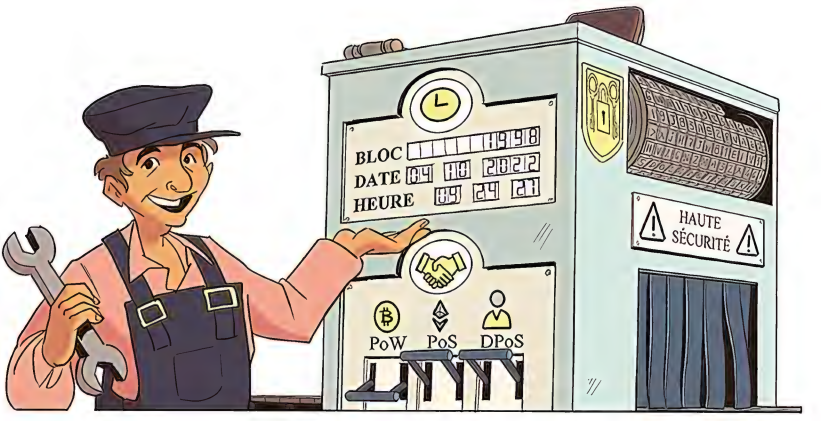


Aujourd'hui, la plupart des plateformes d'échange vous permettent ainsi de passer directement d'une crypto-monnaie à une autre.



CHAPITRE 5

LA TECHNOLOGIE BLOCKCHAIN



L'HISTOIRE DE LA TECHNOLOGIE *BLOCKCHAIN*

Lorsque le système Bitcoin est né, il n'existait aucun concept de « *blockchain* ».

bitcoin ⇨ ₿ JETON CRYPTO-MONNAIE

Bitcoin ⇨ TECHNOLOGIE SOUS-JACENTE

DE MANIÈRE PLUS ÉTENDUE, ELLE EST DÉSORMAIS CONNUE SOUS LE NOM DE TECHNOLOGIE *BLOCKCHAIN*.

2008

PUBLICATION DU *LIVRE BLANC DU BITCOIN*

De par le monde, de grandes institutions financières commencent à s'intéresser à cette technologie sous-jacente au Bitcoin.

2015

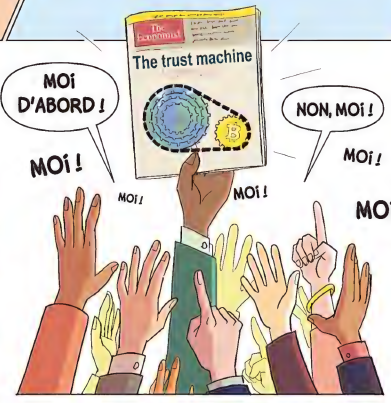
PUBLICATION DE L'ARTICLE « THE TRUST MACHINE » en couverture de *The Economist*

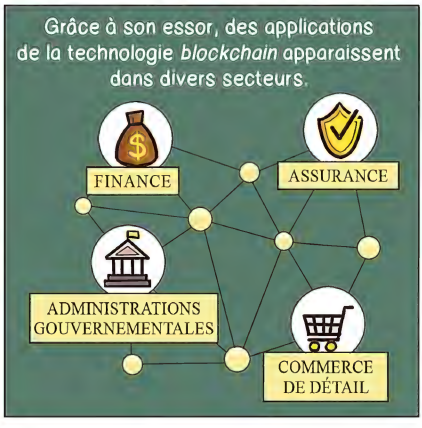
La « machine » *blockchain* devient soudain LA technologie que toute la sphère financière s'arrache.

2016

PREMIERS PLACEMENTS DANS DES SOCIÉTÉS *BLOCKCHAIN*

Depuis, plusieurs milliards de dollars y sont investis chaque année.





BLOCKCHAIN, « LA MACHINE DE CONFIANCE »

La *blockchain* n'est pas une technologie entièrement nouvelle.

ELLE COMBINE EN RÉALITÉ PLUSIEURS SYSTÈMES QUI EXISTENT DÉJÀ TELS QUE LES HORODATAGES...

BLOC
DATE 04 10 2022
HEURE 09 24 21

HAUTE SÉCURITÉ

... LA CRYPTOGRAPHIE ASYMÉTRIQUE...

PoW PoS DPoS

... ET LES ALGORITHMES DE CONSENSUS.

Par exemple, le système Bitcoin associe des horodatages ainsi qu'un mécanisme de « preuve de travail », ou PoW, pour permettre d'éviter les doubles dépenses. Les mineurs doivent pour cela trouver la solution à un problème informatique.

HUM, VOUS AFFIRMEZ VOUS ÊTRE SUFFISAMMENT IMPLIQUÉ DANS LA MAINTENANCE DU RÉSEAU ?

OUI, ET JE PEUX LE PROUVER !

DÉPOSEZ VOTRE BLOC ICI

PoW

L'horodatage inscrit l'instant auquel le bloc est généré...

NOUS ATTESTONS L'ENREGISTREMENT DE VOTRE BLOC CE JOUR À 14 H 36 ET 12 SECONDES.

AU SUIVANT !

BLOC 2350
DATE 16 10 2022
HEURE 14 36 12

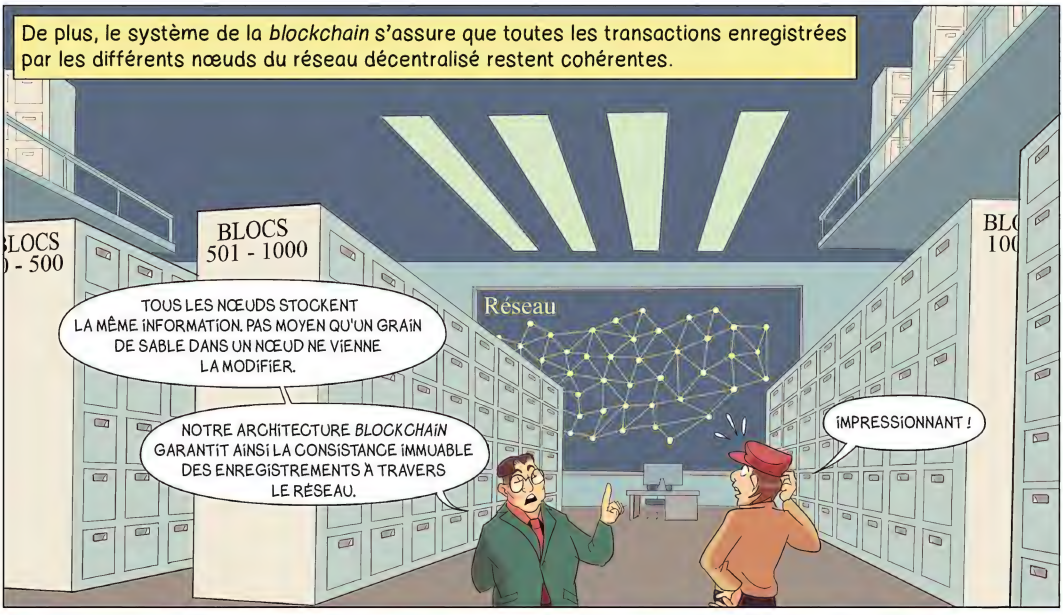
PoW

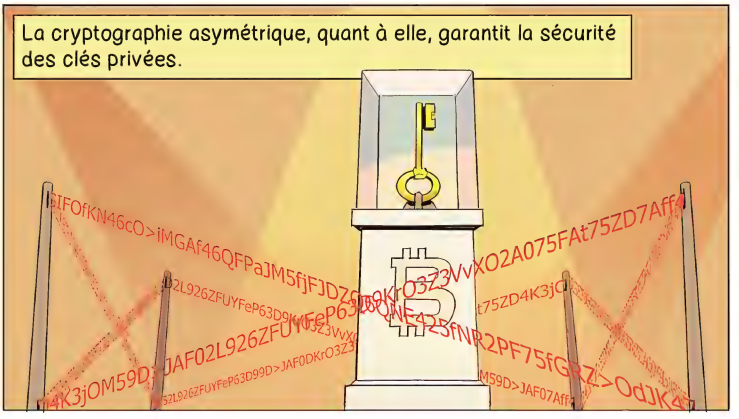
BLOC 2349

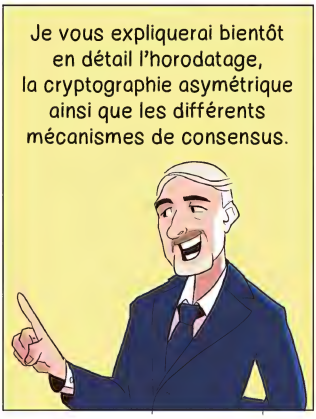
... puis le relie chronologiquement aux autres blocs.

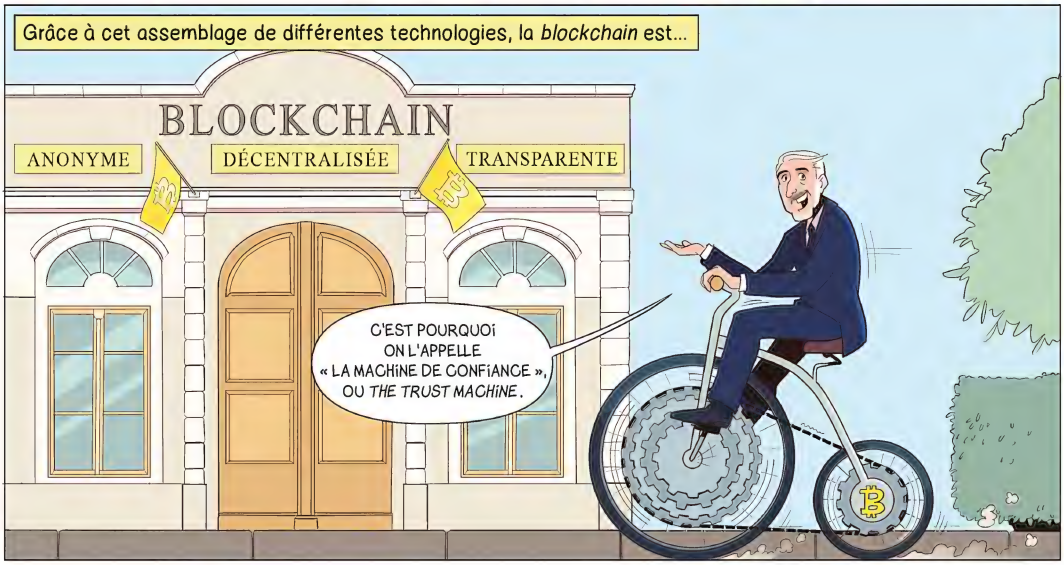
GRÂCE AU POW, POUR UNE QUANTITÉ IDENTIQUE DE TRAVAIL, LES MINEURS ONT LA MÊME CHANCE DE TROUVER EN PREMIER LA BONNE SOLUTION, ET DONC DE RECEVOIR LEUR RÉCOMPENSE.

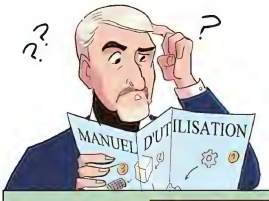
Ce système est dit « équitable ».


De plus, le système de la *blockchain* s'assure que toutes les transactions enregistrées par les différents nœuds du réseau décentralisé restent cohérentes.
BLOCS 501 - 1000
Réseau
TOUS LES NŒUDS STOCKENT LA MÊME INFORMATION. PAS MOYEN QU'UN GRAIN DE SABLE DANS UN NŒUD NE VIENNE LA MODIFIER.
NOTRE ARCHITECTURE *BLOCKCHAIN* GARANTIT AINSI LA CONSISTANCE IMMUABLE DES ENREGISTREMENTS À TRAVERS LE RÉSEAU.
IMPRESSIONNANT !


La cryptographie asymétrique, quant à elle, garantit la sécurité des clés privées.

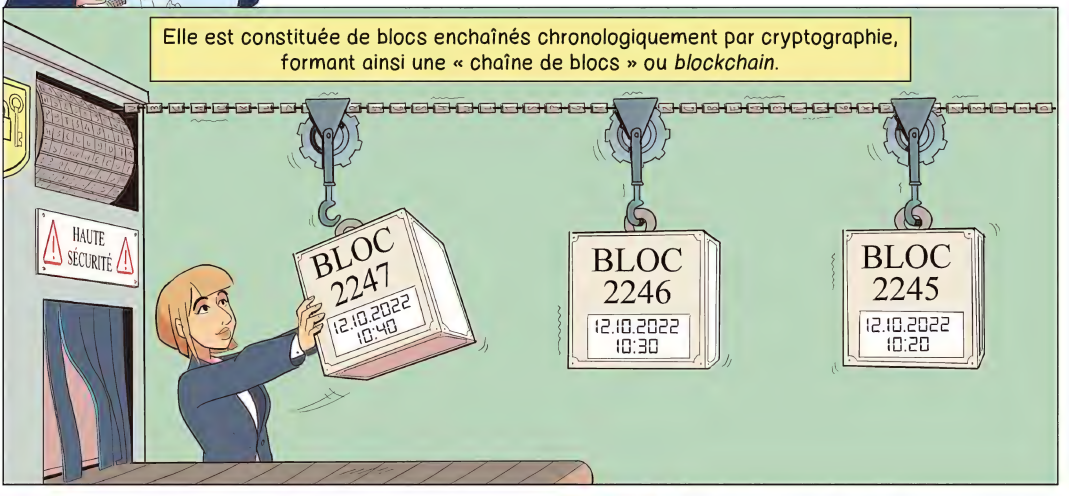

Je vous expliquerai bientôt en détail l'horodatage, la cryptographie asymétrique ainsi que les différents mécanismes de consensus.


Grâce à cet assemblage de différentes technologies, la *blockchain* est...
BLOCKCHAIN
ANONYME
DÉCENTRALISÉE
TRANSPARENTE
C'EST POURQUOI ON L'APPELLE « LA MACHINE DE CONFIANCE », OU *THE TRUST MACHINE*.

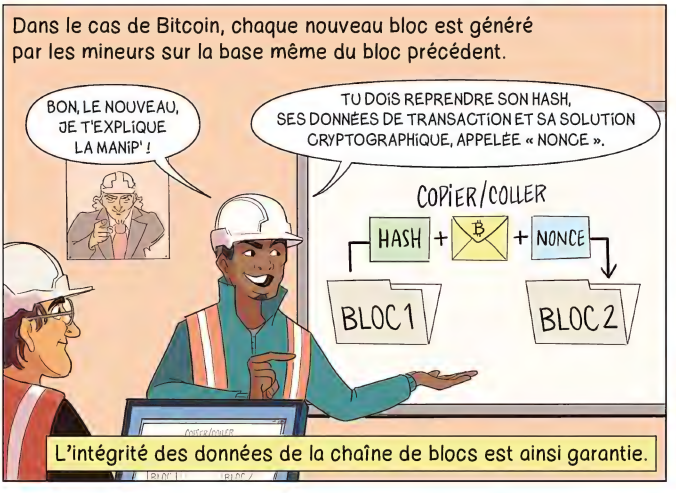


COMMENT FONCTIONNE LA *BLOCKCHAIN* ?

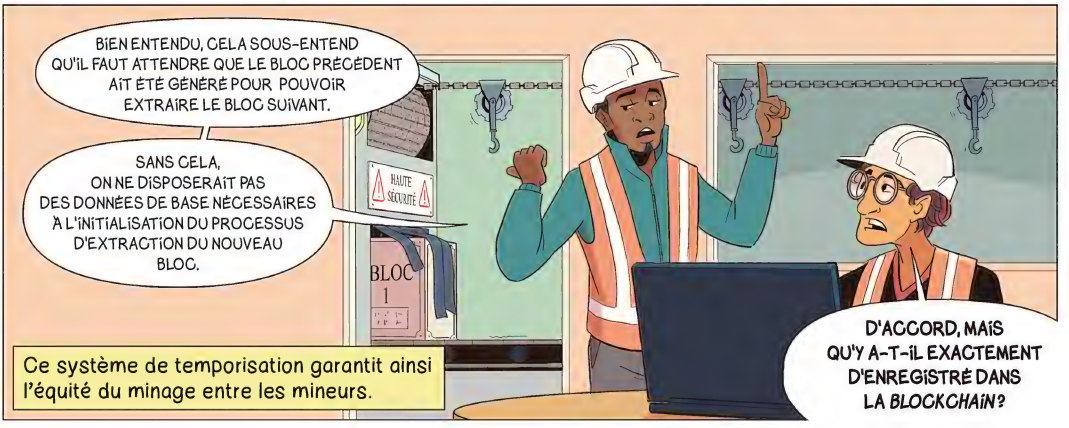
Elle est constituée de blocs enchaînés chronologiquement par cryptographie, formant ainsi une « chaîne de blocs » ou *blockchain*.



Dans le cas de Bitcoin, chaque nouveau bloc est généré par les mineurs sur la base même du bloc précédent.

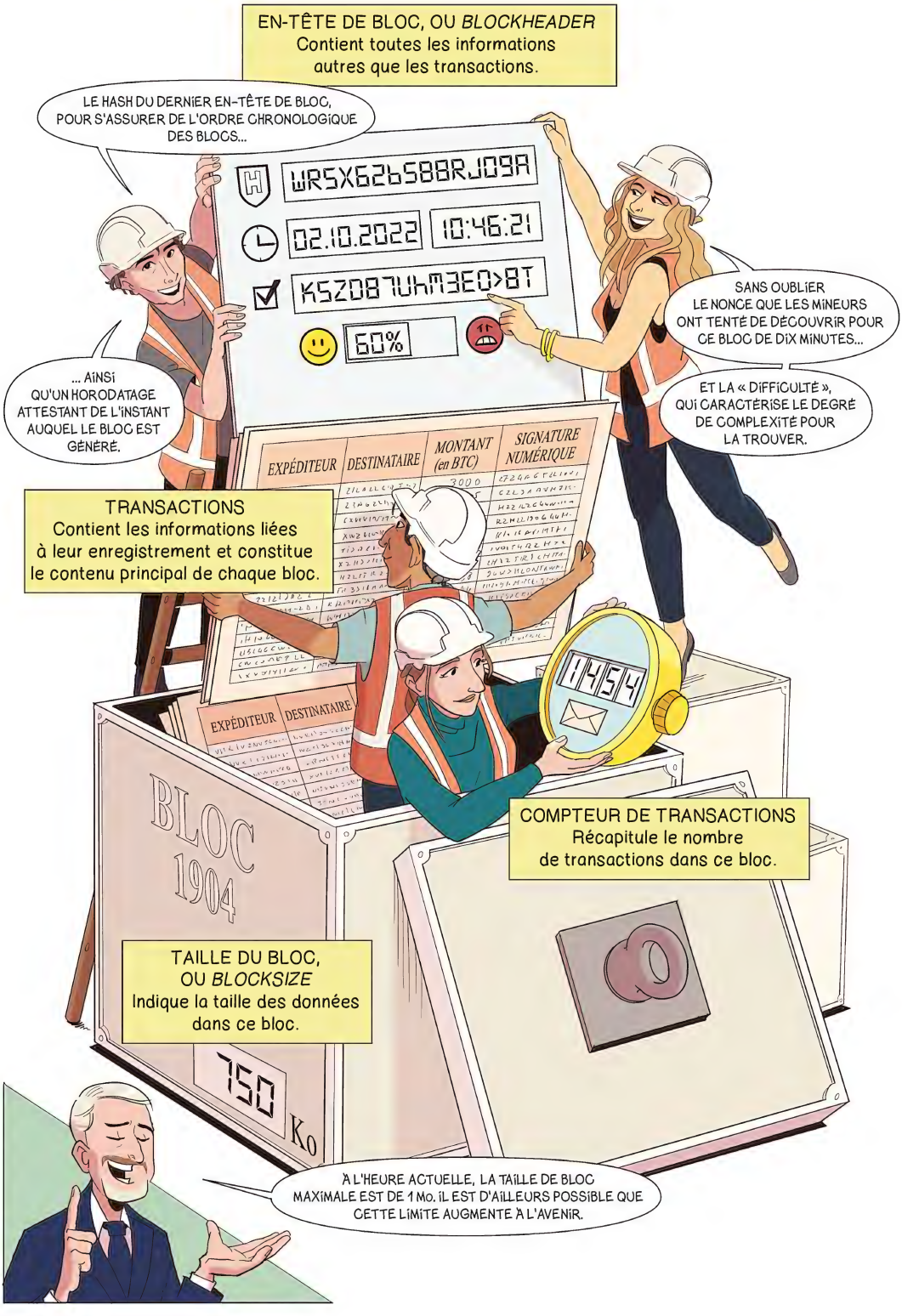


L'intégrité des données de la chaîne de blocs est ainsi garantie.



Ce système de temporisation garantit ainsi l'équité du minage entre les mineurs.

Sur chaque bloc se trouvent des données segmentées en quatre parties.



QU'EST-CE QU'UN HORODATAGE ?

Dans la *blockchain*, l'horodatage, ou *timestamp*, joue le rôle d'un notaire.

JE JURE DE REMPLIR LOYALEMENT MES FONCTIONS EN CONSIGNANT AVEC EXACTITUDE ET PROBITÉ CE QUI SE PASSE SUR LA *BLOCKCHAIN*, ET À QUEL INSTANT!

J'AI MARQUÉ L'HEURE DE CHAQUE TRANSACTION SUR LA *BLOCKCHAIN*...

C'EST BON POUR CE BLOC ! VOUS POUVEZ LE CHAÎNER AUX AUTRES.

Il prouve ainsi que les blocs sont concaténés dans un ordre chronologique.

L'HORODATAGE EST MÊME PLUS FIABLE QU'UN NOTAIRE TRADITIONNEL CAR, UNE FOIS LES INFORMATIONS CONSIGNÉES SUR LA *BLOCKCHAIN*, PERSONNE NE PEUT LES MODIFIER.

CET ENREGISTREMENT EST INVIOLABLE.

Grâce à cette fonction d'horodatage, la technologie *blockchain* convient à des domaines tels que la protection de la propriété intellectuelle.

Par exemple, lorsque vous avez rédigé une thèse, il se peut que vous souhaitiez consulter un expert de l'industrie avant de la publier.

JE NE SAIS PAS, J'HÉSITE... ET SI L'EXPERT S'APPROPRIAIT MON TRAVAIL ?

N'AYEZ CRAINTE !

DANS UN TEL SCÉNARIO, IL VOUS SUFFIT D'ENREGISTRER VOTRE THÈSE SUR LA *BLOCKCHAIN* POUR PROUVER FACILEMENT VOTRE ANTÉRIORITÉ, ET DONC VOTRE PROPRIÉTÉ, SUR CETTE PUBLICATION.

COMMENT LA *BLOCKCHAIN* FAIT-ELLE CONSENSUS ?

Étant donné que tous les mineurs du monde minent simultanément...

... il peut arriver que deux mineurs trouvent la bonne réponse en même temps.

La *blockchain* va alors bifurquer...

HASH 1

HASH 2

... permettant aux autres mineurs de continuer à miner sur l'une ou l'autre de ses deux « fourches ».

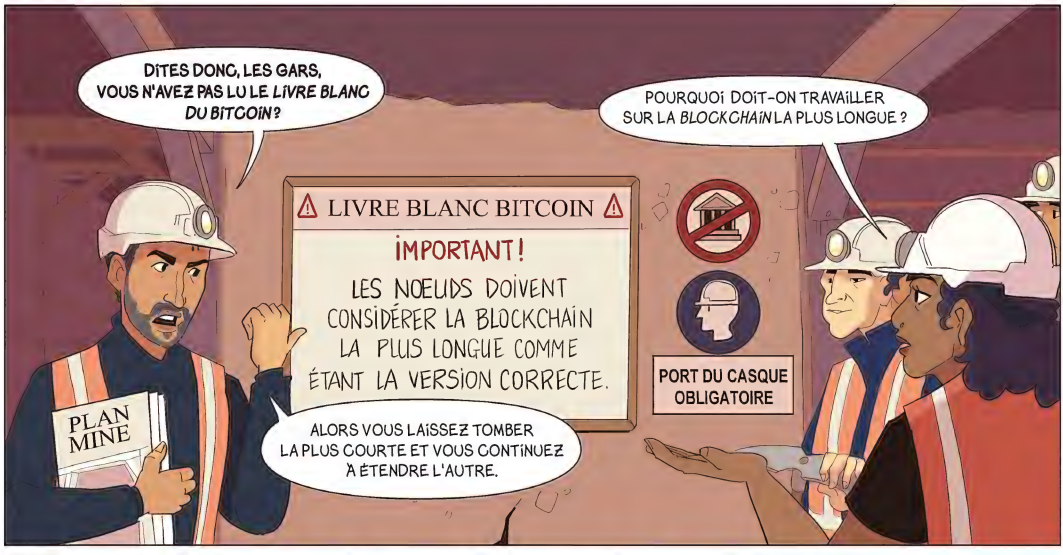
BLOCKCHAIN

MINE

HÉ HÉ ! PETITE INSPECTION SURPRISE !

HASH 1 14

HASH 2 6

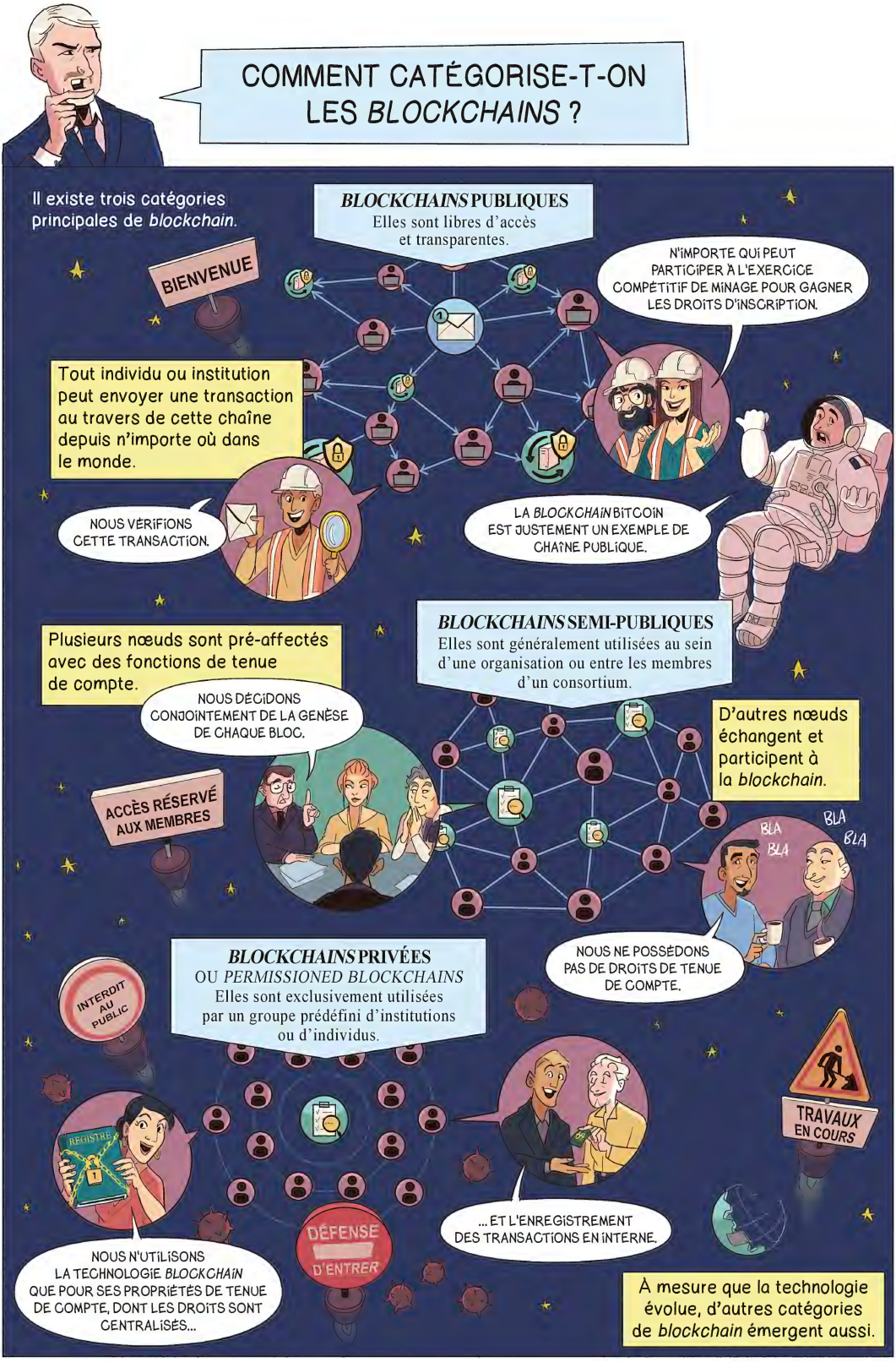

DITES DONC, LES GARS, VOUS N'AVEZ PAS LU LE *LIVRE BLANC DU BITCOIN* ?
POURQUOI DOIT-ON TRAVAILLER SUR LA *BLOCKCHAIN* LA PLUS LONGUE ?
LIVRE BLANC BITCOIN
IMPORTANT !
LES NŒUDS DOIVENT CONSIDÉRER LA BLOCKCHAIN LA PLUS LONGUE COMME ÉTANT LA VERSION CORRECTE.
PORT DU CASQUE OBLIGATOIRE
PLAN MINE
ALORS VOUS LAISSEZ TOMBER LA PLUS COURTE ET VOUS CONTINUEZ À ÉTENDRE L'AUTRE.

Cette approche permet d'une part aux mineurs d'être assurés de ne ne pas continuer à miner sur une version obsolète de la *blockchain*.
OH NON !
???
ZONE CONDAMNÉE POUR OBSOLESCENCE
PLAN MINE
VOUS COMPRENEZ, SI LES JETONS BITCOIN QUI VOUS SONT ENVOYÉS N'ÉTAIENT PAS ENREGISTRÉS SUR LA *BLOCKCHAIN* LA PLUS LONGUE, VOUS POURRIEZ LES PERDRE. LORSQUE LES RAMIFICATIONS LES MOINS LONGUES SONT ABANDONNÉES, L'INFORMATION QUI Y EST STOCKÉE N'EST PLUS MAINTENUE PAR LE SYSTÈME.

D'AUTRE PART, CELA AIDE À MAINTENIR L'UNICITÉ D'UN REGISTRE FIABLE.

D'ACCORD, MAIS QUELLE SOLUTION EXISTE-T-IL POUR ÉVITER CE PROBLÈME DE « FOURCHE » ?

Après le traitement d'une transaction Bitcoin, les mineurs doivent attendre six confirmations de blocs successives pour que la transaction soit véritablement considérée comme validée et définitivement enregistrée.
CONFIRMATIONS


COMMENT CATÉGORISE-T-ON LES *BLOCKCHAINS* ?
Il existe trois catégories principales de *blockchain*.
BIENVENUE
***BLOCKCHAINS* PUBLIQUES**
Elles sont libres d'accès et transparentes.
N'IMPORTE QUI PEUT PARTICIPER À L'EXERCICE COMPÉTITIF DE MINAGE POUR GAGNER LES DROITS D'INSCRIPTION.
Tout individu ou institution peut envoyer une transaction au travers de cette chaîne depuis n'importe où dans le monde.
NOUS VÉRIFIONS CETTE TRANSACTION.
LA *BLOCKCHAIN* BITCOIN EST JUSTEMENT UN EXEMPLE DE CHAÎNE PUBLIQUE.
***BLOCKCHAINS* SEMI-PUBLIQUES**
Elles sont généralement utilisées au sein d'une organisation ou entre les membres d'un consortium.
Plusieurs nœuds sont pré-affectés avec des fonctions de tenue de compte.
NOUS DÉCIDONS CONJOINTEMENT DE LA GENÈSE DE CHAQUE BLOC.
ACCÈS RÉSERVÉ AUX MEMBRES
D'autres nœuds échangent et participent à la *blockchain*.
BLA
BLA
BLA
NOUS NE POSSÉDONS PAS DE DROITS DE TENUE DE COMPTE.
***BLOCKCHAINS* PRIVÉES**
OU *PERMISSIONED BLOCKCHAINS*
Elles sont exclusivement utilisées par un groupe prédéfini d'institutions ou d'individus.
INTERDIT AU PUBLIC
REGISTRE
DÉFENSE D'ENTRER
... ET L'ENREGISTREMENT DES TRANSACTIONS EN INTERNE.
NOUS N'UTILISONS LA TECHNOLOGIE *BLOCKCHAIN* QUE POUR SES PROPRIÉTÉS DE TENUE DE COMPTE, DONT LES DROITS SONT CENTRALISÉS...
TRAVAUX EN COURS
À mesure que la technologie évolue, d'autres catégories de *blockchain* émergent aussi.

CHAPITRE 6

MÉCANISMES DE CONSENSUS ET BIFURCATIONS

QU'EST-CE QUE LE MÉCANISME DE CONSENSUS PAR « PREUVE DE TRAVAIL » ?

Tout d'abord, qu'est-ce qu'un mécanisme de consensus ?

Comme vous le savez, dans la *blockchain*, il n'y a pas d'institution comptable centralisée, telle que les banques, pour assurer la cohérence de chaque transaction.

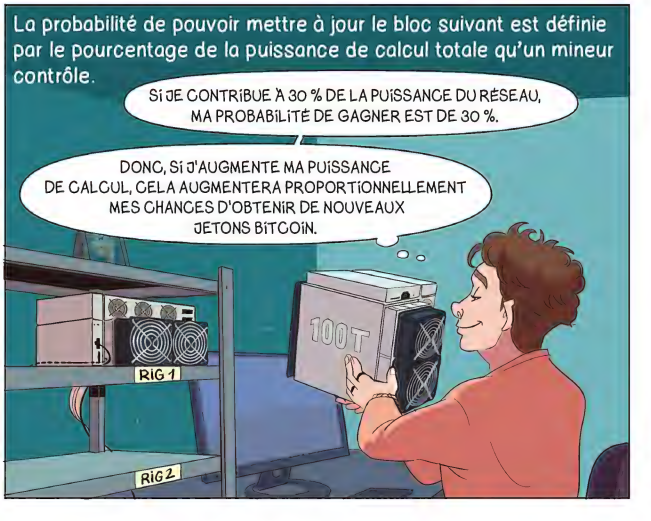
Ce type de mécanisme apporte justement une réponse à cette problématique.

Parmi les principaux qui existent à ce jour, on peut citer la « preuve de travail », ou PoW pour *proof of work*.

Ce mécanisme mesure les efforts générés par les mineurs pour déterminer leur probabilité de recevoir une récompense.

Plus ces efforts sont productifs, plus les chances d'obtenir une récompense de bloc sont élevées.

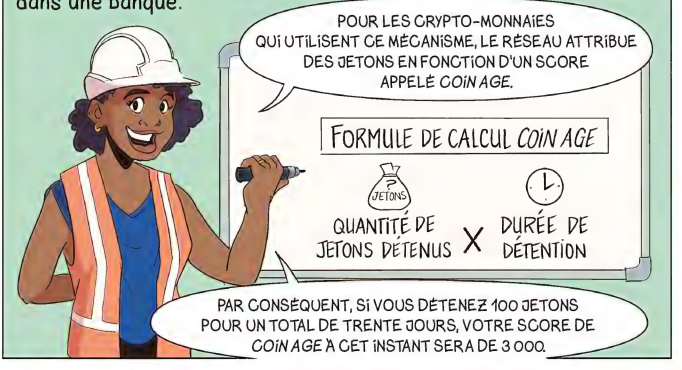
La probabilité de pouvoir mettre à jour le bloc suivant est définie par le pourcentage de la puissance de calcul totale qu'un mineur contrôle.



QU'EST-CE QUE LE MÉCANISME DE CONSENSUS PAR « PREUVE D'ENJEU » ?

Aussi appelée PoS pour *proof of stake*, elle détermine la puissance minière en examinant la quantité de jetons détenue par un mineur, et sur quelle durée.

Ainsi, les intérêts sont calculés comme pour un dépôt d'argent dans une banque.

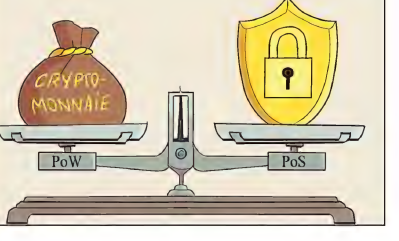


La PoS présente deux avantages par rapport à la preuve de travail :

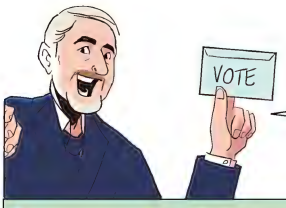
Sur la *blockchain*, la validation des opérations est basée sur le consensus de la majorité des mineurs.

Donc, si un mineur peu scrupuleux veut passer en force et faire adopter des transactions qu'il prétend « valides »...

À l'heure actuelle, de nombreuses crypto-monnaies utilisent un système hybride combinant la preuve de travail pour émettre de nouveaux jetons et la preuve d'enjeu pour le maintien de la sécurité du réseau.

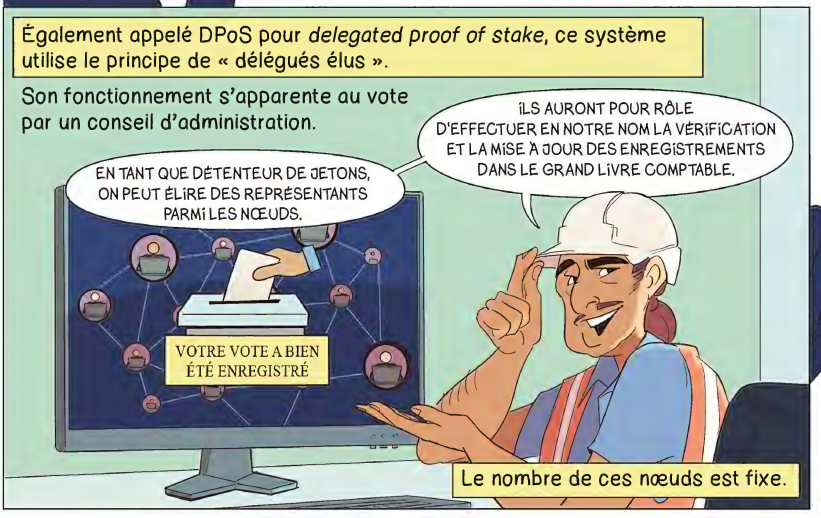


QU'EST-CE QUE LA « PREUVE D'ENJEU DÉLÉGUÉE » ?



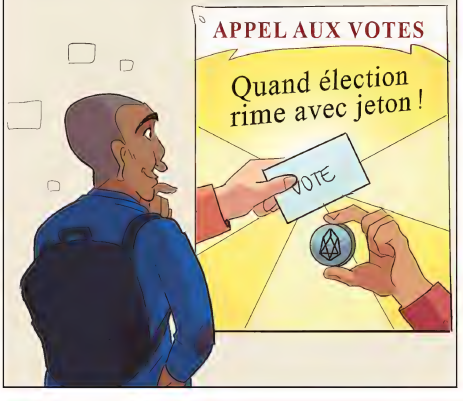
Également appelé DPoS pour *delegated proof of stake*, ce système utilise le principe de « délégués élus ».

Son fonctionnement s'apparente au vote par un conseil d'administration.



BitShares, PPCoin, et quelques autres crypto-monnaies utilisent aussi ce type de consensus.

Pour encourager une plus grande participation à ces élections, le réseau génère une petite quantité de jetons en récompense.



Une fois élus...

Par rapport à la PoW, la DPoS a considérablement augmenté la capacité de traitement des données de *blockchain*, en permettant aux transactions d'être effectuées en quelques secondes.

QU'EST-CE QUE LA « PREUVE À DIVULGATION NULLE DE CONNAISSANCE » ?

Aussi nommé ZKP pour *zero knowledge proof*, ce système permet à un « prouveur » d'attester à un « vérificateur » qu'une déclaration donnée est vraie...

... SANS POUR AUTANT AVOIR À LUI RÉVÉLER L'INFORMATION ELLE-MÊME. C'EST FORT, NON ?

COMMENT EST-CE POSSIBLE ? RIEN DE MAGIQUE, IL S'AGIT D'UNE TECHNIQUE DE CRYPTAGE !

Prenons un exemple simple...

A VEUT PROUVER À B QU'ELLE POSSÈDE LA CLÉ PERMETTANT D'OUVRIR UNE PIÈCE.

A

B

BIEN ENTENDU, CETTE PIÈCE NE PEUT ÊTRE DÉVERROUILLÉE QU'AVEC LA CLÉ EN QUESTION.

En suivant la méthode traditionnelle...

TU N'AS QU'À ME REMETTRE TA CLÉ. JE POURRAI AINSI DÉVERROUILLER MOI-MÊME LA PIÈCE ET AVOIR LA CONFIRMATION QUE C'EST BIEN LA BONNE QUE TU DÉTIENS.

HOULÀ, C'EST RISQUÉ POUR MOI ! SI JE TE REMETS LA CLÉ, QUI ME DIT QUE TU NE VAS PAS EN PROFITER ?

En utilisant le principe ZKP...

JE TE PROPOSE PLUTÔT DE DÉVERROUILLER MOI-MÊME LA PIÈCE AVEC MA CLÉ...

... PUIS DE TE MONTRER UN SIMPLE OBJET DONT TU SAIS PERTINEMMENT QU'IL NE PEUT PROVENIR QUE DE LA PIÈCE EN QUESTION.

Ainsi, ce mécanisme résout efficacement de nombreux problèmes liés à la vérification et à la confidentialité lors de transactions.

GRÂCE À LUI, IL EST FACILE DE PROUVER QUE L'ON CONNAÎT LE MOT DE PASSE D'UN COMPTE, SANS POUR AUTANT AVOIR À EN TRANSMETTRE L'INFORMATION.

PAR EXEMPLE, SI LE COMPTE A UN SOLDE DE 327 564,52 €, JE N'AI QU'À DONNER LE DERNIER CHIFFRE DES CENTIMES, À SAVOIR 2, POUR PROUVER QUE J'Y AI BIEN ACCÈS.

À L'HEURE ACTUELLE, LA CRYPTO-MONNAIE ZCASH ASSURE DES TRANSACTIONS HAUTEMENT ANONYMES AVEC CE SYSTÈME.

QU'EST-CE QUE L'ALGORITHME DE HACHAGE ?

C'est un algorithme de cryptographie qui traite du chiffrement.

Cette fonction mathématique permet de transformer une information complexe en une petite chaîne de caractères très réduite, sans moyen « intuitif » de reconnaître le signal initial.

La taille de cette chaîne d'octets est fixe.

L'ALGORITHME DE HACHAGE SÉCURISÉ UTILISÉ PAR BITCOIN EST LE SHA-256. IL PERMET DE GÉNÉRER UNE CHAÎNE AYANT UNE TAILLE DE 32 OCTETS, SOIT 256 CARACTÈRES BINAIRES.

CE QUI, UNE FOIS CONVERTI EN LANGAGE HEXADÉCIMAL, CORRESPOND À UNE SUITE DE 64 CARACTÈRES, COMPOSÉE DE CHIFFRES ET DE LETTRES.

Cette chaîne est comparable à une empreinte dont l'algorithme SHA-256 garantit le caractère UNIQUE !

Une modification, même mineure, de la donnée d'entrée changerait complètement la valeur de hachage obtenue en sortie.

Ainsi, l'entrée initiale est la seule qui permette d'obtenir la même chaîne en sortie.

En plus de permettre de stocker un plus grand nombre de données sur la *blockchain*, cette compression simplifie grandement le processus d'identification.

Une autre particularité propre à l'algorithme de hachage est d'être à sens unique.

SA FONCTION EST DE CHIFFRER, PAS DE DÉCHIFFRER !

ENCRYPTE

65dsR24FGF1
D85V5F7R69
GD457T6fY4j
G78tR5Hj13K

IL N'EXISTE DONC PAS DE FORMULE ANALYTIQUE ENTRE LES DONNÉES D'ENTRÉE ET LES CHAÎNES EN SORTIE.

MAIS S'IL N'EXISTE PAS DE FORMULE POUR INVERSER LE PROCESSUS, CELA VEUT-IL DIRE QU'IL EST IMPOSSIBLE DE RECONSTITUER UNE VALEUR D'ENTRÉE SUR LA BASE DE LA CHAÎNE EN SORTIE ?

Le seul moyen de déchiffrer le signal d'entrée correspondant, ou *hash value*, est de tâtonner.

PARTONS D'UNE IMAGE SIMPLE GÉNÉRÉE PAR HACHAGE ET DONT LA RÉSOLUTION EST 3 X 3 PIXELS.

LA SEULE MANIÈRE DE RETROUVER L'IMAGE ORIGINALE QUI FAISAIT À LA BASE 4 X 3 PIXELS EST DE TESTER UN PAR UN LE COLORIAGE, OU NON, DES 12 CARRÉS, CE QUI REPRÉSENTE 4 096 COMBINAISONS POSSIBLES.

IMAGE HACHÉE EN 3 x 3

MAIS C'EST ÉNORME ! J'IMAGINE MÊME PAS LE TEMPS QUE ÇA VA PRENDRE !

IMAGE ORIGINALE EN 4 x 3

A B C D

4 096 POSSIBILITÉS

Imaginez maintenant le nombre d'essais qu'il faudrait pour une image avec une résolution de 1 500 x 2 500 pixels !

Ainsi, dans le cadre de l'extraction des bitcoins, les mineurs ne peuvent pas tricher pour trouver la solution avant les autres. Ils n'ont d'autre choix que de...

... S'IMPLIQUER ET TESTER SANS RELÂCHE DES VALEURS DE HASH POUR ÊTRE LE PREMIER À TROUVER LA SOLUTION PERMETTANT DE RECEVOIR DES JETONS BITCOIN EN RÉCOMPENSE.

138E ESSAI

Cette méthode est appelée « attaque par force brute ».

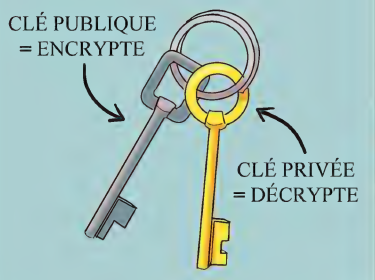
Grâce au caractère aléatoire de cet effort, chaque mineur a autant de chances de tomber au hasard le premier sur la bonne solution.

IMPARTIAL

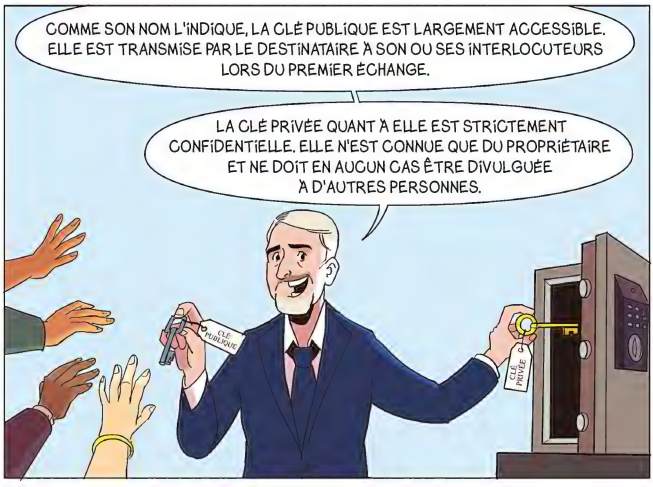
ÉQUITABLE

QU'EST-CE QUE LA CRYPTOGRAPHIE ASYMÉTRIQUE ?

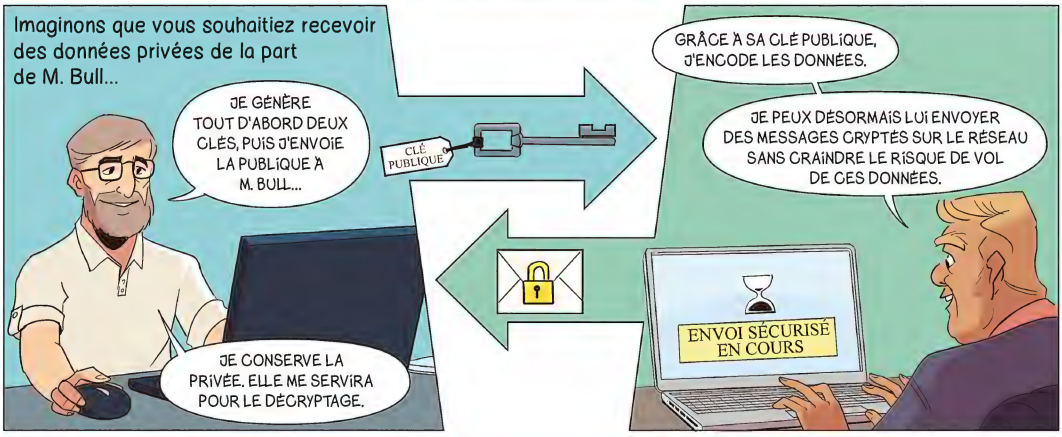
Elle utilise la même paire de clés pour le chiffrement et le déchiffrement.



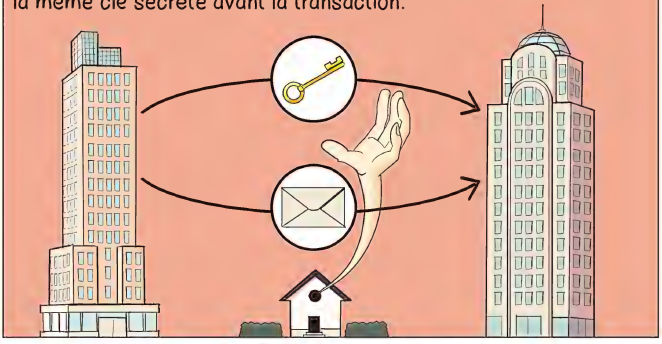
Celle-ci est propre à chaque utilisateur.



Les messages chiffrés à l'aide de la clé publique ne peuvent être déchiffrés que par la clé privée associée.



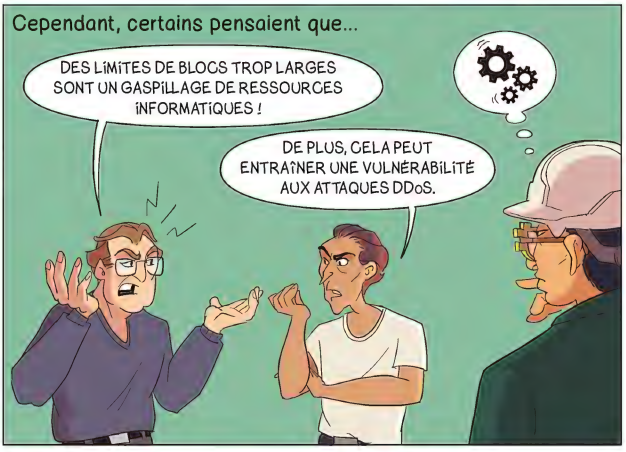
La cryptographie asymétrique est donc plus sécurisée que les algorithmes à clé symétrique où les deux parties partagent la même clé secrète avant la transaction.



POURQUOI BITCOIN DOIT-IL SE METTRE À L'ÉCHELLE ?

Lorsque Bitcoin a été initialement créé, Satoshi NAKAMOTO n'avait pas l'intention de limiter la taille de blocs.

Cependant, certains pensaient que...



Ainsi, pour assurer la sécurité et la stabilité du réseau Bitcoin, Satoshi NAKAMOTO se ravisa.

À l'époque, il n'y avait qu'un petit nombre d'utilisateurs, avec un petit volume de transactions...

Mais depuis 2013, le prix de Bitcoin a considérablement augmenté ainsi que le nombre d'utilisateurs, entraînant une congestion du réseau.

Face à cette augmentation constante du volume d'échanges de Bitcoin, le réseau a eu du mal à traiter rapidement les enregistrements de transactions.

Ce phénomène entraîna également une hausse des frais de transaction.

La communauté Bitcoin décida donc de réagir.

Elle commença à envisager de mettre à l'échelle le système.

IL FAUT QUE L'ON METTE À JOUR NOTRE PROPRE CODE, DE MANIÈRE À AUGMENTER NOTRE CAPACITÉ À GÉRER LES TRANSACTIONS. QUELLES SOLUTIONS PROPOSEZ-VOUS ?

ET SI ON AUGMENTAIT LA LIMITE DE TAILLE DE BLOC ?

SUPPRIMONS PLUTÔT LES INFORMATIONS REDONDANTES DE BLOC.

CETTE CAPACITÉ D'UN SYSTÈME À S'ADAPTER EN CAS DE FORTE CROISSANCE DE LA DEMANDE POUR MAINTENIR SA PERFORMANCE EST APPELÉE LA SCALABILITÉ, OU « MISE À L'ÉCHELLE ».

Malgré les nombreuses solutions proposées depuis 2013, aucune n'a été largement acceptée.

Par conséquent, la question de l'évolutivité du Bitcoin reste un sujet très controversé.

Le 24 août 2017, une mise à niveau du protocole Bitcoin, appelée SegWit pour *segregated witness*, fut implémentée au bloc 481 824 très exactement.

WOUAHO !
GRÂCE À ELLE, LA CAPACITÉ DE TRAITEMENT DES DONNÉES D'UN SEUL BLOC A ÉTÉ MULTIPLIÉE PAR 1,7 !

MISE À JOUR RÉALISÉE AVEC SUCCÈS !

Une deuxième tentative de changement de protocole appelée SegWit2X, ou B2X, suivit mais elle ne suscita pas l'adhésion de la communauté Bitcoin et fut vite abandonnée.

SegWit est un changement de protocole destiné à augmenter la capacité de la *blockchain*.

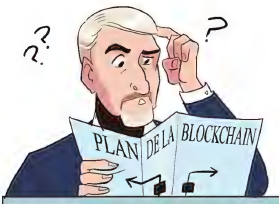
INITIALEMENT, CHAQUE BLOC ENREGISTRAIT NON SEULEMENT TOUS LES DÉTAILS DES TRANSACTIONS, MAIS AUSSI CEUX PERMETTANT DE VÉRIFIER LA LÉGITIMITÉ DE CHACUNE D'ELLES TELS QUE...

- L'HORODATAGE
- LES JETONS BITCOIN TRANSFÉRÉS
- LA SIGNATURE NUMÉRIQUE DE LA TRANSACTION

OR, IL S'AVÈRE QUE L'UTILISATEUR RÉGULIER NE S'INTÉRESSE QU'À LA QUANTITÉ D'ACTIFS QU'IL A DANS SES COMPTES, ET NON À CHAQUE TRANSACTION.

En partant de ce constat, SegWit proposa de supprimer les informations de signature numérique dans un bloc pour ainsi laisser plus de place aux données liées aux transactions.

Après Bitcoin, SegWit fut implémentée sur d'autres crypto-monnaies telles que Litecoin et Bitcoin Gold.



QU'EST-CE QU'UNE BIFURCATION DE *BLOCKCHAIN* ?

Dans un système centralisé, il est très simple d'effectuer des mises à jour logicielles.

Dans un système de *blockchain* décentralisé, la mise à jour n'est pas une tâche facile.

N'ayant pas d'autorité centrale pour mettre à niveau le protocole, la communauté Bitcoin doit faire appel au consensus.

Réussir à établir un consensus dans un réseau décentralisé comme celui du Bitcoin n'est pas chose facile.

S'il n'y a pas une adhésion suffisante, c'est précisément là qu'une bifurcation, aussi appelée *fork*, se produit.

Conformément au nouveau protocole créé en parallèle à la branche originelle de la *blockchain*...

Étant donné que ces jetons sont reçus sans avoir à être payés, ils sont parfois appelés des « bonbons », ou *candies*.

En fonction du degré d'adoption de la bifurcation, certains jetons seront amenés à prendre une véritable valeur, tandis que d'autres resteront à l'état de simple *candies*.

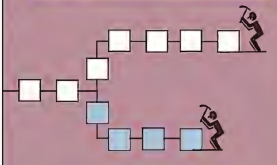
Pour qu'une bifurcation ait lieu et qu'elle survive, il faut réussir à fédérer un nombre élevé de mineurs.

Au cours des quatre derniers mois de l'année 2017, le système Bitcoin a continué de tester de nombreuses bifurcations, donnant ainsi naissance à de (trop) nombreux (re)jetons.

QUELLE DIFFÉRENCE ENTRE UNE BIFURCATION MINEURE ET UNE BIFURCATION MAJEURE ?

Une bifurcation de *blockchain* peut être classifiée comme...

MAJEURE, ou *hard fork*



MINEURE, ou *soft fork*

BTC ORIGINEL

BTC1 BIFURCATION

Dans le cas de bifurcations majeures, après la modification du protocole Bitcoin, les anciens nœuds rejettent les blocs créés par de nouveaux nœuds.

Ainsi, les mineurs suivent la règle d'origine, créant un nouveau bloc à la suite du dernier bloc vérifié.

Dans le cas de bifurcations mineures, les anciens nœuds n'ont pas la capacité de détecter la modification du protocole Bitcoin.

Les mineurs peuvent ainsi travailler sur des blocs qu'ils n'ont pas intégrés ou validés.

Cependant, ces deux bifurcations ont une caractéristique commune : elles restent rétrocompatibles.

Le nouveau protocole accepte le code produit par l'ancienne version.

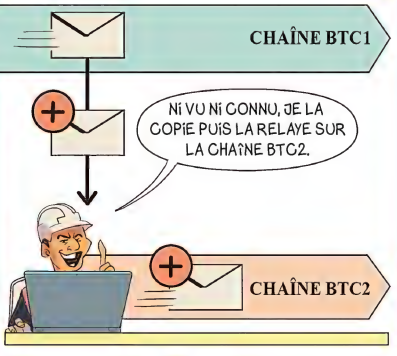
Lorsque le réseau Bitcoin fait face à une bifurcation, le plus grand risque auquel est confronté un utilisateur lambda est une...

Lorsque le réseau Bitcoin se divise en différentes versions, chaque détenteur de jetons bitcoin conserve ses avoirs sur la chaîne principale.

Cela implique qu'une transaction diffusée sur une chaîne peut être réutilisée frauduleusement par un nœud sur l'autre chaîne et ainsi recevoir une validation indue.

Imaginons par exemple que vous souhaitiez acheter une voiture électrique avec vos jetons stockés sur la chaîne BTC1.

Si le système n'est pas bien verrouillé, un nœud malhonnête peut usurper la transmission envoyée vers BTC1.



Ainsi, une fois les deux transactions validées sur leur chaîne respective, l'usurpateur peut profiter du fruit de la transaction indûment acquise...

LA BIFURCATION ENTRE ETHEREUM ET ETHEREUM CLASSIC

C'est une étude de cas exemplaire de bifurcation majeure.

Tout commence en mai 2016 avec le lancement officiel du projet DAO, ou *decentralized autonomous organization*.

The DAO

Organisation autonome décentralisée

L'OBJECTIF EST DE CONSTITUER UN FOND DE CAPITAL-RISQUE SOUS LA FORME D'UNE PLATEFORME DE FINANCEMENT PARTICIPATIF.

LA GOUVERNANCE EST AUTONOME, DÉCENTRALISÉE ET AUTOMATISÉE GRÂCE AUX CONTRATS INTELLIGENTS ETHEREUM QUI LA RÉGISSENT.

JE VOUS EXPLIQUERAI TRÈS PROCHAINEMENT CE QU'EST UN CONTRAT INTELLIGENT.

On peut comparer le fonctionnement d'une DAO à celle d'une coopérative ou d'une société par actions.

La gouvernance y est exercée démocratiquement par les membres.

CHAQUE DÉCISION, CHAQUE PROJET ET CHAQUE DÉPENSE SONT SOUMIS À UN VOTE COLLECTIF.

CONTRAT INTELLIGENT

Les membres sont l'équivalent d'actionnaires.

POUR DEVENIR MEMBRE, IL FAUT INVESTIR DE L'ARGENT DANS L'ORGANISATION EN ÉCHANGE DE JETONS.

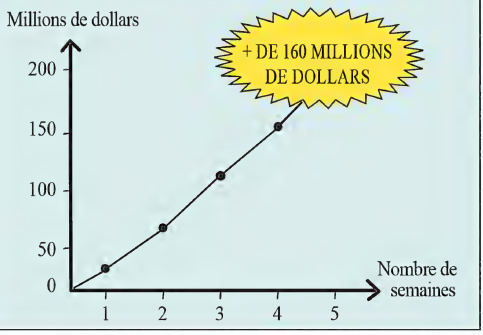
NOTRE RÉMUNÉRATION EST PROPORTIONNELLE À LA VALEUR DE NOTRE CONTRIBUTION.

Ils se sont regroupés au sein de la DAO pour répondre à un objectif commun...

AIDER LES CRÉATEURS À LANCER LEUR PROJET ETHEREUM EN LES ÉVALUANT ET EN DÉCIDANT COLLECTIVEMENT DE LEUR FINANCEMENT, OU NON.

PROJET 70 % 30 %

Ainsi, le projet DAO put lever en moins d'un mois...



Malheureusement, DAO disparut quelques mois plus tard à la suite d'une attaque d'un hacker survenue le 17 juin 2016.

OUAÏP ! J'AI EXPLOITÉ LES FAILLES DES CONTRATS INTELLIGENTS ET AINSI DÉROBÉ L'ÉQUIVALENT DE **50 MILLIONS DE DOLLARS EN JETONS ETHEREUM.**

Afin de pouvoir récupérer les actifs des investisseurs spoliés, la communauté Ethereum vota pour modifier le code du protocole Ethereum.

C'EST AINSI QUE LE PROTOCOLE ETHEREUM BIFURQUA AU BLOC N° 199 000.

199 000

200 000

200 000

200 001

200 002

CETTE BIFURCATION PERMIT D'ANNULER LES TRANSACTIONS ETHEREUM EFFECTUÉES DEPUIS CE BLOC, Y COMPRIS CELLES DES HACKERS.

Cependant, certains s'en offusquèrent...

CETTE MESURE VIOLE LES PRINCIPES FONDAMENTAUX DE DÉCENTRALISATION ET D'IMMUABILITÉ DE LA *BLOCKCHAIN* !

NOUS INSISTONS POUR CONTINUER À EXPLOITER LA CHAÎNE D'ORIGINE.

... Et deux *blockchains* se formèrent.

ETC

ETH

D'un côté, la chaîne Ethereum Classic, ou ETC.

NOUS NE RECONNAISSONS PAS LES TRANSACTIONS QUI ONT ÉTÉ ANNULÉES.

REJOIGNEZ ETC

De l'autre, la chaîne Ethereum, ou ETH.

NOUS, SI !

ETH

CHACUN DES DEUX PROTOCOLES REPRÉSENTE AINSI UN CONSENSUS ET DES VALEURS COMMUNAUTAIRES DIFFÉRENTS.

Une personne qui détenait un jeton Ether avant la bifurcation détient donc ensuite à la fois un jeton ETC et un jeton ETH.

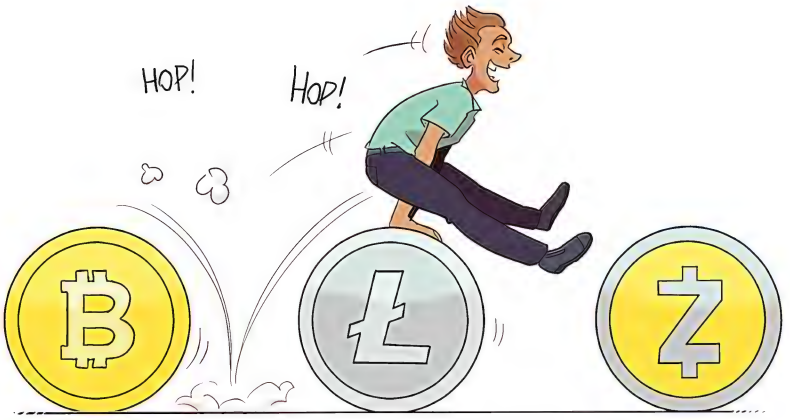
TROP BIEN ! J'AI DEUX JETONS POUR LE PRIX D'UN.

VOUS AVEZ UN NOUVEAU JETON !

ETC + ETH

CHAPITRE 7

APPLICATIONS DE LA BLOCKCHAIN : LES CRYPTO-MONNAIES



QU'EST-CE QU'UNE CRYPTO-MONNAIE ?

De nos jours, il existe quatre principaux types de projets de *blockchain*.

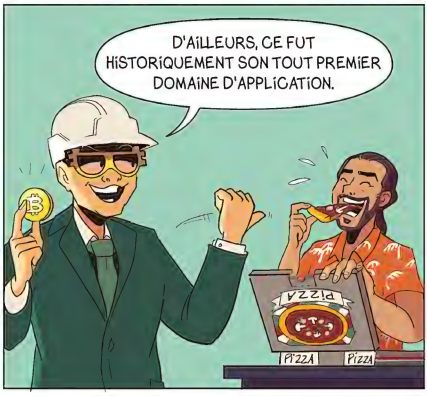
CRYPTO-MONNAIES

PLATEFORMES

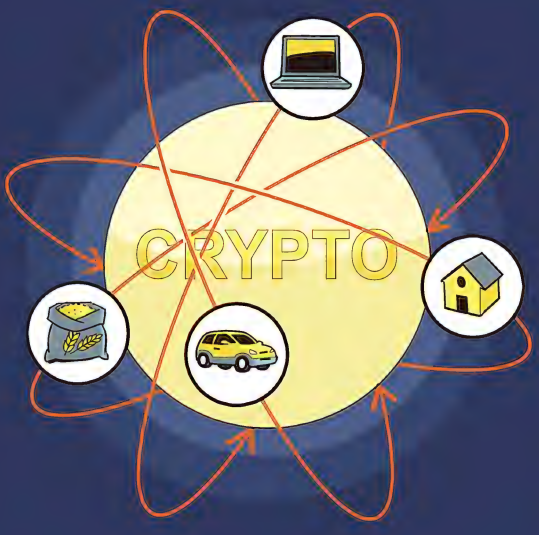
JETONS UTILITAIRES
ou *utility tokens*

JETONS D'ACTIFS
ou *asset tokens*

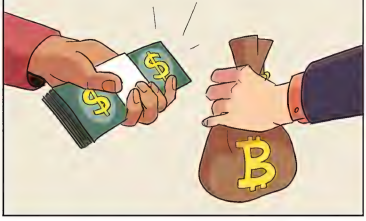
Elles sont le domaine d'application principal de la *blockchain*.



Les crypto-monnaies sont des moyens d'échange dans le monde de la *blockchain*.



Elles servent d'intermédiaire lors de transactions de biens de valeurs équivalentes, par exemple de l'or, de l'argent, ou encore des billets de banque.



À l'heure actuelle, il existe plus de 1 000 actifs de *blockchain* sur le marché.

Parmi les crypto-monnaies les plus connues, on peut citer...

BITCOIN

NEM

LITECOIN

ZCASH

DASH

MONERO

LE DASH, LE MONERO ET LE ZCASH SONT DES CRYPTO-MONNAIES DITES « ANONYMES ». ELLES PERMETTENT LE RÈGLEMENT DES PAIEMENTS TOUT EN PRÉSERVANT L'IDENTITÉ DES DEUX PARTIES.

De nouvelles crypto-monnaies naissent tous les jours.

Depuis des années maintenant, Bitcoin a la plus grande capitalisation boursière de l'ensemble des crypto-monnaies.

1

CAPITALISATION BOURSIÈRE DES CRYPTO-MONNAIES

LES CRYPTO-MONNAIES ONT PLUSIEURS CARACTÉRISTIQUES PROPRES.

TRANSNATIONALITÉ

ANONYMAT

REGISTRE DISTRIBUÉ

NON-RÉPLICABILITÉ

CARACTÉRISTIQUE #1 : LA TRANSNATIONALITÉ

Que ce soit grâce au *World Wide Web* ou au travers d'un réseau local, les crypto-monnaies ne sont pas limitées par des frontières.

Elles prospèrent sur Internet et peuvent être envoyées partout où celui-ci est accessible.

MÊME EN VIVANT DANS L'ESPACE !!

Comparés aux méthodes traditionnelles, les frais de transaction pour l'envoi de crypto-monnaies partout dans le monde sont très bas.

CRYPTO STORE

AUPARAVANT, L'ENVOI DE JETONS BITCOIN NE COÛTAIT QU'UN DIXIÈME DE MILLIÈME DE BTC. C'EST PLUS CHER MAINTENANT.

BITCOIN 0,0002 BTC

BITCOIN CASH 0,0001 BCC

DASH 0,002 DASH

ETHEREUM 0,01 ETH

CONCRÈTEMENT, APRÈS CONVERSION, COMBIEN CELA COÛTE-T-IL ?

SEULEMENT QUELQUES DIZAINES DE DOLLARS, MÊME POUR DES TRANSACTIONS TRÈS IMPORTANTES.

De plus, les transferts de crypto-monnaies sont également plus rapides.

EN RÈGLE GÉNÉRALE, IL SUFFIT DE PLUSIEURS MINUTES À UNE HEURE POUR EFFECTUER UN TRANSFERT.

TEMPS DE TRANSFERT ESTIMÉ : 10 MINUTES

CARACTÉRISTIQUE #2 : L'ANONYMAT

L'anonymat est une caractéristique notable des crypto-monnaies.

PERSONNE NE PEUT SAVOIR LA QUANTITÉ D'ACTIFS QUE JE POSSÈDE, OU BIEN AVEC QUI J'EFFECTUE DES TRANSACTIONS.

Il existe différents niveaux d'anonymat.

POTION D'INVISIBILITÉ

PANOPLIE DU PARFAIT ANONYME

Faites votre choix !

BASIQUE

AVANCÉ

EXTRÊME

TU VOIS, L'ANONYMAT DU SYSTÈME BITCOIN EST AU NIVEAU LE PLUS ÉLÉMENTAIRE.

POURQUOI ÉLÉMENTAIRE ? MÊME SI N'IMPORTE QUI A ACCÈS AUX ENREGISTREMENTS DE TRANSACTIONS SUR LA *BLOCKCHAIN*, PERSONNE NE SAIT QUI SE CACHE DERRIÈRE LES ADRESSES DES CONTREPARTIES ?

BASIQUE

12.10.2022 TRANSACTION EXP:

24.09.2022 TRANSACTION EXP:

06.08.2022 TRANSACTION EXP:

OUI, MAIS SI UNE PERSONNE DÉCOUVRE TON ADRESSE BITCOIN, ELLE PEUT ALORS ACCÉDER À TOUS LES ENREGISTREMENTS DE TRANSACTIONS IMPLIQUANT CETTE ADRESSE...

... ET AINSI TENTER D'EN DÉDUIRE LA QUANTITÉ DES ACTIFS ASSOCIÉS.

ARGH!

Dash et Monero offrent des niveaux d'anonymat plus élevés.

ZUT ! MÊME SI J'AI DÉCOUVERT QUI SE CACHE DERRIÈRE CETTE ADRESSE, JE N'AI TOUJOURS PAS ACCÈS AUX ENREGISTREMENTS DE TRANSACTIONS !!

FACTURE

LISTE COURSES

FAN #1

I LOVE YOU LADY GAGA

PRESSE

LADY GAGA

COMPTA

Quant à Zcash, il fait passer l'anonymat à un niveau encore supérieur.

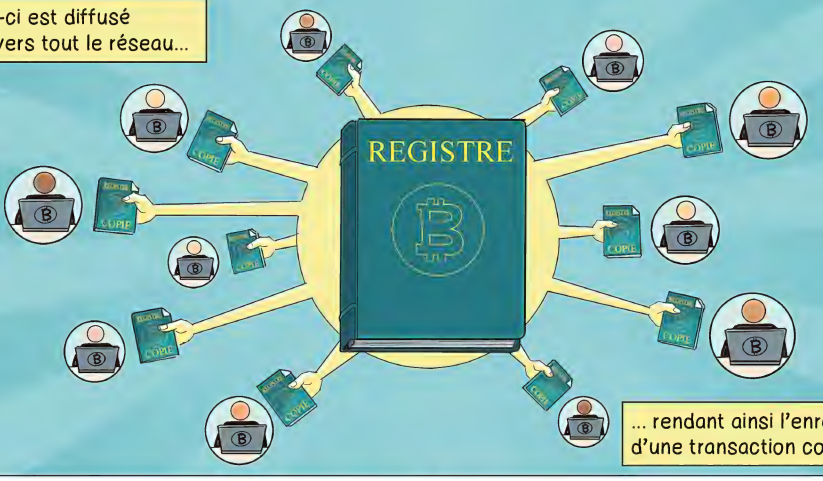
SEUL CELUI QUI POSSÈDE LA CLÉ PRIVÉE PEUT CONSULTER LES ENREGISTREMENTS DE TRANSACTIONS.

Les crypto-monnaies anonymes Dash, Monero et Zcash permettent le règlement des paiements tout en préservant l'identité des deux parties grâce au processus de « preuve à divulgation nulle de connaissance », ou *zero-proof knowledge*.

CARACTÉRISTIQUE #3 : LE REGISTRE DISTRIBUÉ

Les crypto-monnaies utilisent un grand livre de registre distribué, ou *distributed ledger*.

Celui-ci est diffusé à travers tout le réseau...



... rendant ainsi l'enregistrement d'une transaction cohérent.

Ce grand registre de comptes distribué permet à l'expéditeur et au destinataire d'une même transaction de consulter leur enregistrement sur le réseau.

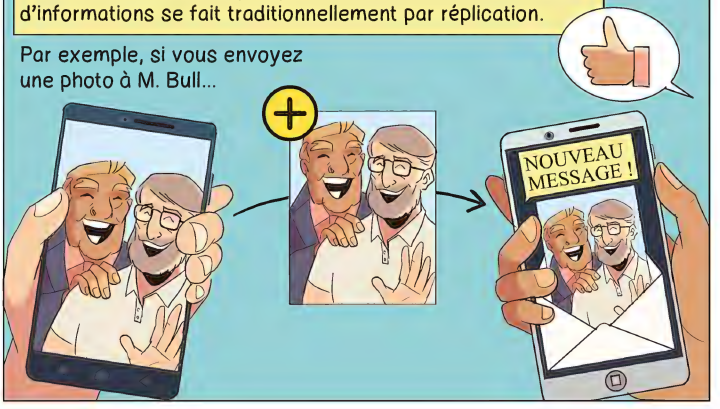
Par exemple, si vous transférez 0,5 bitcoin à M. Bull...

Grâce à ce système transparent et équitable...

CARACTÉRISTIQUE #4 : LA NON-RÉPLICABILITÉ

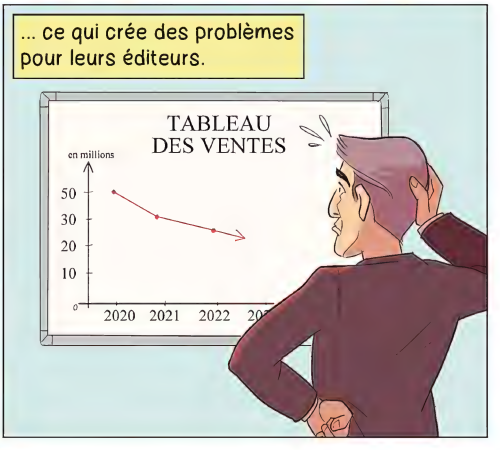
Dans le monde numérique qu'est celui d'Internet, la diffusion d'informations se fait traditionnellement par réplication.

Par exemple, si vous envoyez une photo à M. Bull...

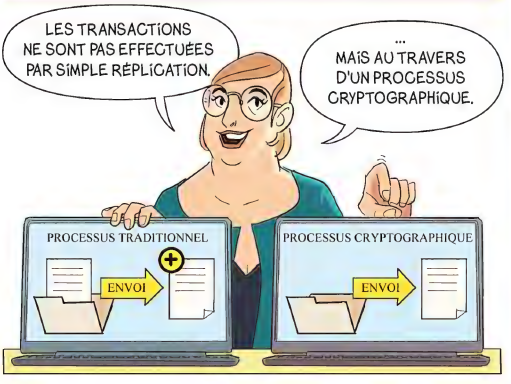


Cette facilité à dupliquer numériquement les textes, images et vidéos est un problème majeur dans la violation du droit d'auteur...

... ce qui crée des problèmes pour leurs éditeurs.



L'une des principales raisons pour lesquelles les crypto-monnaies peuvent être considérées comme de véritables actifs vient du fait qu'elles ne peuvent pas être dupliquées.



Cette propriété fondamentale de non-réplicabilité est la caractéristique clé qui permet justement aux crypto-monnaies d'être l'objet de transactions.

QU'EST-CE QUE LE LITECOIN ?

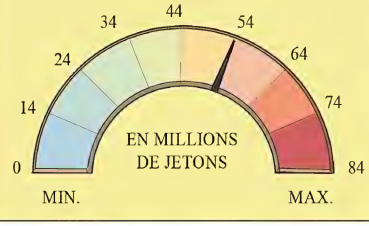
La crypto-monnaie Litecoin, ou LTC en abrégé, a été créée par Charlie LEE le 9 novembre 2011.

Par conséquent, Litecoin partage de nombreuses similitudes avec Bitcoin.

	LITECOIN	BITCOIN	LTC *vs* BTC
Offre totale	84 millions de jetons	21 millions de jetons	x 4
Récompense de bloc	divisée par 2 tous les 4 ans		=
Mécanisme de consensus	preuve de travail		=
Vitesse de confirmation de blocs	2,5 min. pour un bloc	10 min. pour un bloc	x 4

Semblable à Bitcoin, sa récompense de bloc est divisée par deux tous les quatre ans.

En 2018, l'émission totale de litecoins en était déjà à 54 millions de jetons.



Bitcoin demeure à ce jour le favori incontesté des investisseurs : sa notoriété est due notamment à son ancienneté et à son degré d'adoption mondial.

QU'EST-CE QUE LE NEM ?

MIAM!

Le NEM, acronyme pour *New Economy Movement*, a été créé le 1er avril 2015.

C'est la première crypto-monnaie à avoir été construite à l'aide d'un développement piloté par des tests...

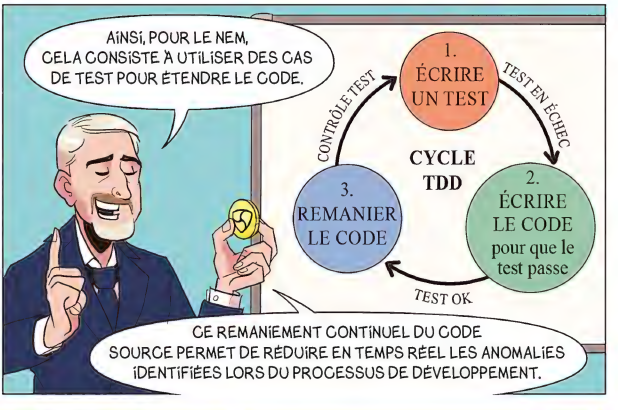
... c'est-à-dire que le code a été conçu pas à pas.

REGARDE, VOICI UNE ANALOGIE TRÈS SIMPLE.

LORS DE LA CONSTRUCTION D'UNE MAISON, LES MAÇONS UTILISENT UN FIL À PLOMB COMME GUIDE POUR POSER LES BRIQUES, AFIN DE S'ASSURER QUE LE MUR EST BIEN DROIT.

Si les briques étaient posées immédiatement, sans test en continu, il pourrait y avoir un risque de mauvais alignement, difficilement récupérable une fois le mur terminé.

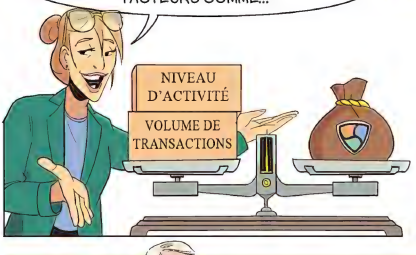
AINSI, POUR LE NEM, CELA CONSISTE À UTILISER DES CAS DE TEST POUR ÉTENDRE LE CODE.



CE REMANIEMENT CONTINUEL DU CODE SOURCE PERMET DE RÉDUIRE EN TEMPS RÉEL LES ANOMALIES IDENTIFIÉES LORS DU PROCESSUS DE DÉVELOPPEMENT.

Comparé à Bitcoin et à Litecoin, le système NEM adopte un mécanisme de consensus spécifique appelé « preuve de l'importance », ou « PoI ».

CELUI-CI DÉTERMINE LA DISTRIBUTION DES RÉCOMPENSES EN FONCTION DE PLUSIEURS FACTEURS COMME...



La fréquence de confirmation de blocs est de 60 secondes.

WOUAOH !

C'EST CONSIDÉRABLEMENT PLUS RAPIDE QUE BITCOIN ET LITECOIN !

L'offre totale est plafonnée à 9 milliards de jetons.

MAIS CETTE OFFRE A ÉTÉ ÉMISE EN TOTALITÉ DÈS LA VENTE INITIALE DE JETONS.

AINSI, AUCUNE RÉCOMPENSE DE BLOC N'EST GÉNÉRÉE POUR CHAQUE NOUVEAU BLOC ENREGISTRÉ SUR LA *BLOCKCHAIN*.

Les récompenses de minage se limitent donc aux frais de transaction, ce qui rend évidemment le processus moins attractif pour ceux qui n'ont pas participé à la souscription initiale de jetons.

QU'EST-CE QUE LE DASH ?

La crypto-monnaie anonyme Dash fait ses débuts le 1er janvier 2014.

Son système propose trois options de transaction.

Standard

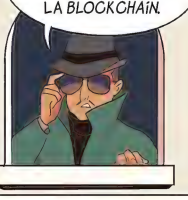
ELLE EST SIMILAIRE À CELLE DU BITCOIN.

InstantX

LES TRANSACTIONS SONT TRAITÉES EN QUELQUES SECONDES, CAR LES MINEURS NE SONT PAS MIS EN CONCURRENCE.

100 % anonyme

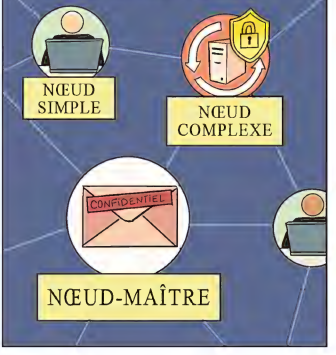
LES TRANSACTIONS ENTRE PARTICIPANTS NE PEUVENT PAS ÊTRE RETRACÉES *VIA* LA *BLOCKCHAIN*.



CETTE TROISIÈME OPTION OFFRE AUX UTILISATEURS UN DEGRÉ D'ANONYMAT SUPÉRIEUR À BITCOIN.

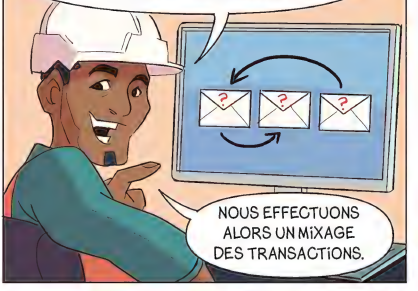
PAR QUEL PROCÉDÉ DASH EFFECTUE-T-IL LES TRANSACTIONS ANONYMES ?

Il utilise des nœuds-maîtres, ou *master-nodes*, en plus des nœuds réguliers.



Les *master-nodes* offrent une série de fonctionnalités telles que la réalisation de transactions anonymes et instantanées.

TOUTE PERSONNE SOUHAITANT EFFECTUER DES TRANSACTIONS ANONYMES NOUS SOUMET UNE DEMANDE.



NOUS EFFECTUONS ALORS UN MIXAGE DES TRANSACTIONS.

Après ce mixage, le réseau n'est donc plus en mesure de déterminer les parties impliquées dans la transaction, garantissant ainsi leur anonymat.

Pour illustrer simplement ce principe de mixage...

PRENONS PAR EXEMPLE TROIS PERSONNES. C'EST EN RÈGLE GÉNÉRALE LE NOMBRE DE TRANSACTIONS QUI SONT MIXÉES ENTRE ELLES.

CHAQUE PERSONNE A DÉPOSÉ SON ARGENT SUR LA TABLE.

JE MÉLANGE LEUR MONNAIE...

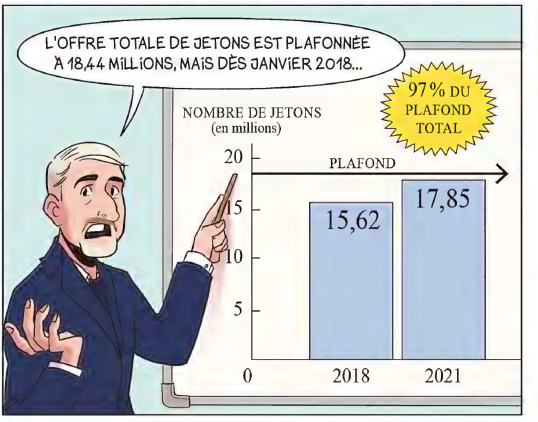
... PUIS CHACUNE D'ELLES REPREND LE MÊME MONTANT QU'ELLE AVAIT INITIALEMENT DÉPOSÉ.

Ainsi, personne ne peut connaître l'origine exacte de chaque nouvelle pile de monnaie.

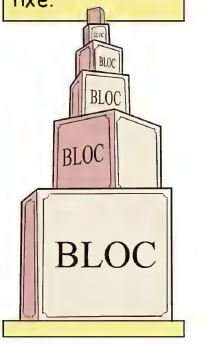
QU'EST-CE QUE LE MONERO ?

Cette crypto-monnaie anonyme, dont l'acronyme est XMR, est née le 18 avril 2014.

Seulement trois mois après Dash !



Monero n'a pas de taille de bloc fixe.



Grâce à un mécanisme de signatures d'anneau* aussi appelées « signatures de cercle », il permet l'anonymat des transactions.

* Ou *ring signature*.

Ce système est similaire à celui des pétitions conjointes utilisées dans la Chine ancienne.

L'identité de la personne à l'origine de la pétition était protégée par le fait que toutes les signatures étaient inscrites en forme d'anneau circulaire, sans aucune indication d'antériorité.

L'identité de l'initiateur reste ainsi cachée.

Dans le cadre de Monero...

Le réseau se charge de mixer la clé publique du signataire avec une autre clé publique, avant de signer un message.

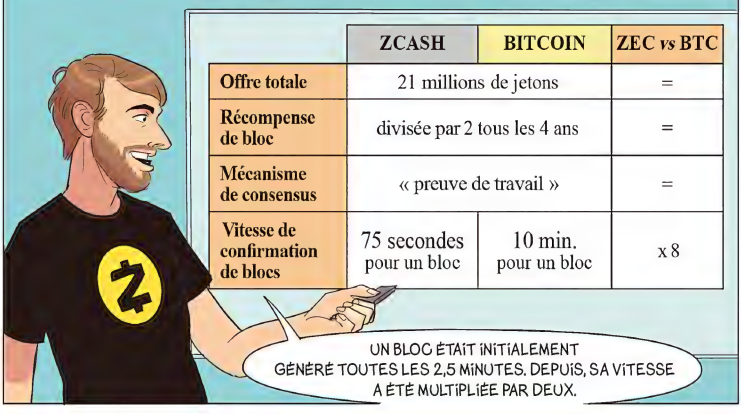
De plus, Monero permet de masquer l'adresse du destinataire à l'expéditeur, ainsi que de masquer l'identité de l'expéditeur au destinataire.

QU'EST-CE QUE LE ZCASH ?

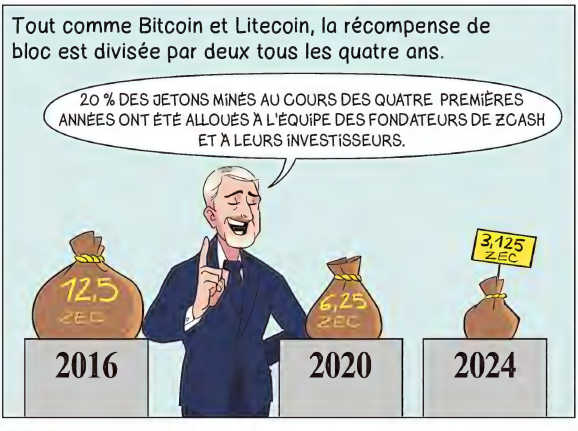
Le système anonyme Zcash, également connu sous le nom de Zero Cash ou ZEC, a été créée par Zooko WILCOX le 28 octobre 2016.

Son code source partage de nombreuses similitudes avec Bitcoin.

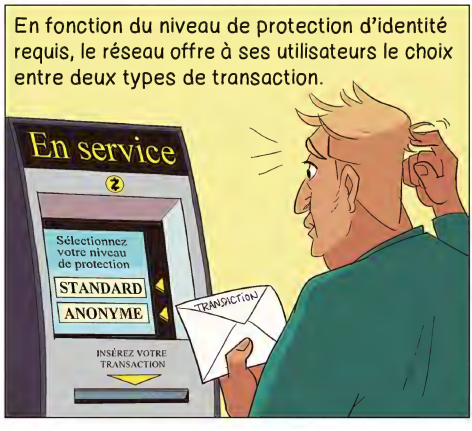
	ZCASH	BITCOIN	ZEC *vs* BTC
Offre totale	21 millions de jetons		=
Récompense de bloc	divisée par 2 tous les 4 ans		=
Mécanisme de consensus	« preuve de travail »		=
Vitesse de confirmation de blocs	75 secondes pour un bloc	10 min. pour un bloc	x 8



Tout comme Bitcoin et Litecoin, la récompense de bloc est divisée par deux tous les quatre ans.



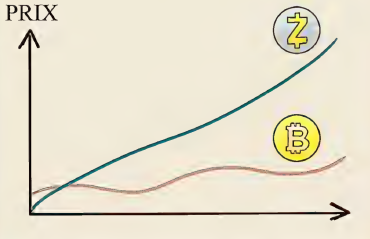
En fonction du niveau de protection d'identité requis, le réseau offre à ses utilisateurs le choix entre deux types de transaction.



Lors de son lancement, le protocole Zcash s'est concentré sur l'amélioration des fonctions d'anonymat de Bitcoin.

Cette fonctionnalité fit véritablement sensation au sein de la communauté *blockchain*.

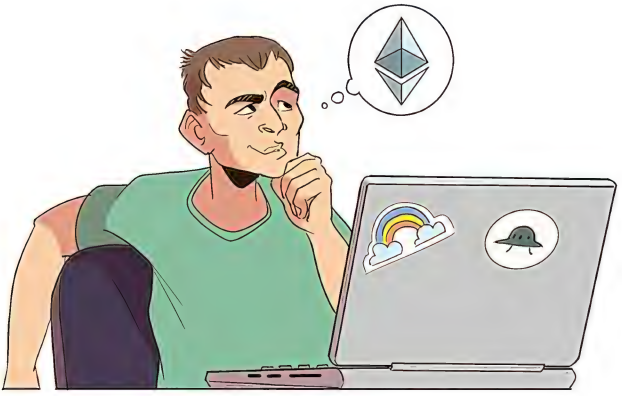
Ce qui entraîna, à ses débuts, une augmentation de prix sept fois supérieure à celle du bitcoin.



À l'heure actuelle, le délai d'exécution pour les transactions anonymes sur le système Zcash est assez important : environ vingt minutes.

CHAPITRE 8

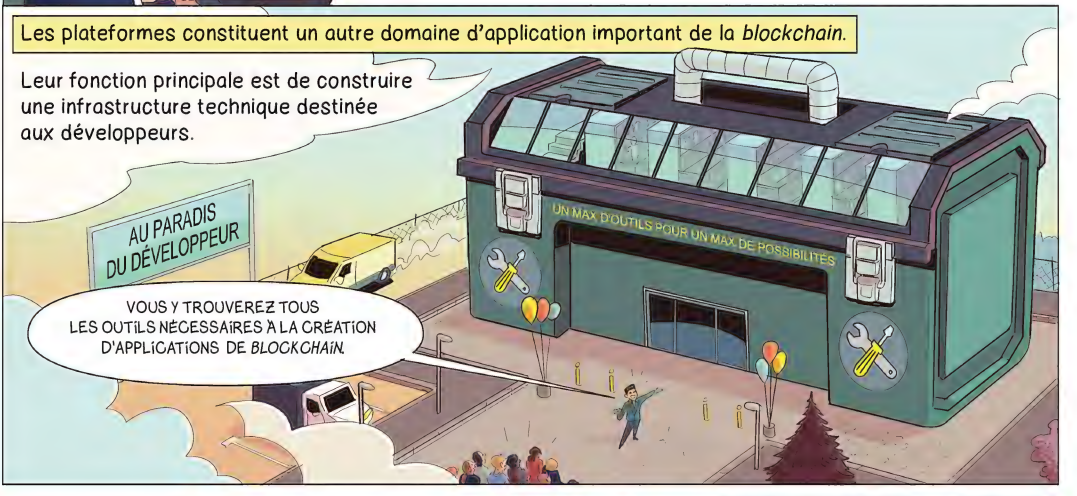
APPLICATIONS DE LA BLOCKCHAIN : PLATEFORMES, TOKENISATION



QU'EST-CE QU'UNE PLATEFORME ?

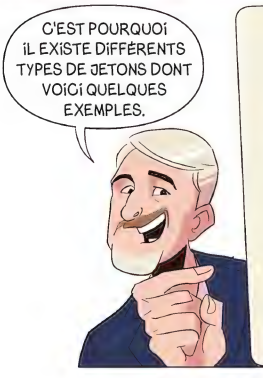
Les plateformes constituent un autre domaine d'application important de la *blockchain*.

Leur fonction principale est de construire une infrastructure technique destinée aux développeurs.



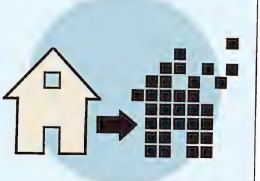
Parmi les applications possibles, on peut citer l'émission de jetons numériques, ou *tokens*.

Cette représentation d'un actif réel en jeton numérique, aussi appelée « tokenisation », permet son utilisation et son échange sur une *blockchain*.



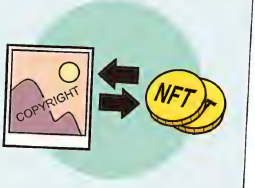
JETON UTILITAIRE
OU *UTILITY TOKEN*

Permet l'échange de services ou de produits.



JETON D'ACTIFS
OU *ASSET TOKEN*

Permet la tokenisation de biens réels.



JETON NON FONGIBLE
OU *NON FUNGIBLE TOKEN* (NFT)

Permet l'échange de droit de propriété sur des images numériques.

L'écriture de contrats intelligents, ou *smart contracts*.

Ce sont des codes informatiques qui opèrent sur une *blockchain* et dont le rôle est de faciliter l'exécution des termes d'un contrat.

AVEC MOI, C'EST RAPIDE ET SANS BAVURE ! UNE FOIS LES RÈGLES DÉFINIES, L'EXÉCUTION EST AUTOMATIQUE. J'ATTENDS JUSTE LE BON MOMENT POUR ENTRER EN ACTION.

Par exemple, un contrat intelligent pour un bail de location peut être transcrit sur une *blockchain*.

Comme pour un protocole traditionnel, les clauses de l'accord entre les parties sont définies dans le contrat intelligent.

CONTRAT INTELLIGENT

Lorsque le propriétaire reçoit le paiement du loyer...

... et permet de délivrer la clé de l'appartement au locataire.

AGENCE DE LOCATION

... le contrat s'exécute automatiquement...

La clé peut être remise par la délivrance d'un digicode, la reconnaissance faciale ou *fingerprint* automatiquement activée, l'activation à distance d'un système d'ouverture de type Intratone (avec badge physique/activation par téléphone) ou d'un badge Vigik.

Grâce à ces contrats intelligents...

FINI LES LOURDEURS ADMINISTRATIVES !

FORMULAIRE

FRAIS EN SUS

+0,012 BTC

- ☑ Gestion automatisée
- ☑ Transactions rapides et sécurisées
- ☑ Coût moindre, pas d'intermédiaire

Ils évitent également les risques dus à la malhonnêteté d'un interlocuteur.

UN NOMBRE CONSIDÉRABLE DE PLATEFORMES DE CONTRATS INTELLIGENTS SONT ACTUELLEMENT EN COURS DE DÉVELOPPEMENT.

DEPUIS JANVIER 2018, LA PLATEFORME LA PLUS UTILISÉE EST ETHEREUM.

ethereum

Grâce aux plateformes *blockchain*, c'est tout un écosystème qui se crée. Des applications vivent et meurent au gré des projets qui y sont développés.

QU'EST-CE QUE ETHEREUM ?

Le système Ethereum a été créé fin 2013 par Vitalik BUTERIN, un programmeur russo-canadien âgé d'à peine 20 ans.

Le jeton de la plateforme est appelé ether, avec l'acronyme ETH, ou gas.

Puis, en juillet 2014...

ÇA Y EST, J'AI PUBLIÉ LE *LIVRE BLANC POUR ETHEREUM* !

LANCEMENT CAMPAGNE ICO

Nom du projet : ETHEREUM

LOADING

GRÂCE À LUI, JE VAIS POUVOIR FAIRE CONNAÎTRE MON PROJET SUR LE RÉSEAU *BLOCKCHAIN* ET COMMENCER LA PRÉVENTE DE MA NOUVELLE CRYPTO-MONNAIE.

À cette époque, ce type de prévente, appelé ICO (pour *initial coin offering*), était assez en vogue auprès de la communauté crypto.
Je vous expliquerai bientôt en détail son fonctionnement.

Au cours d'une période de souscription de 42 jours...

BONNE NOUVELLE ! PLUS DE 60 MILLIONS DE JETONS ETHER ONT DÉJÀ ÉTÉ PRÉVENDUS EN ÉCHANGE DE BITCOINS.

GRÂCE À CELA, NOUS AVONS PU LEVER PLUS DE 30 000 BTC !

9,9 % DE CE MONTANT ONT ÉTÉ REVERSÉS AUX PREMIERS SOUTIENS ET AUTANT AUX DÉVELOPPEURS IMPLIQUÉS, EN AMONT DE CETTE CAMPAGNE DE FINANCEMENT PARTICIPATIF.

60 102 216 ETH

9,9 % 1ers soutiens

9,9 % développeurs

Ainsi, Ethereum comprenait au moment de son lancement une quantité totale de plus de 72 millions de jetons.

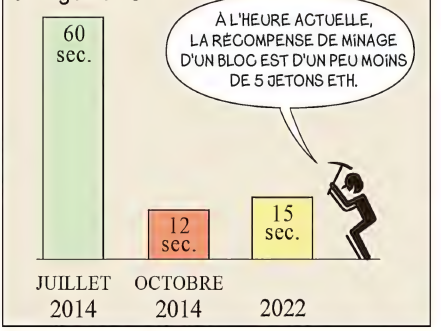
Comme Bitcoin, le système Ethereum est décentralisé.

Le registre est ouvert, transparent et immuable, et sa mise à jour effectuée par l'ensemble du réseau.

IL ADOPTE ÉGALEMENT LE MODÈLE DE CONSENSUS PAR PREUVE DE TRAVAIL.

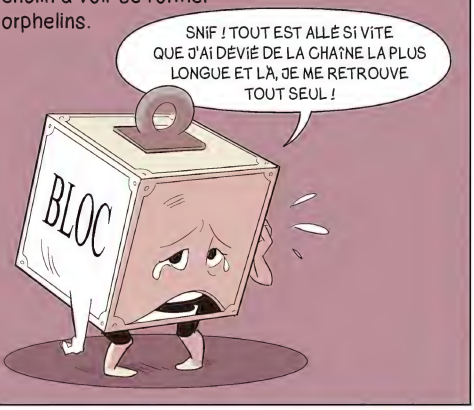
26 % DU TOTAL DES JETONS ÉMIS NOUS SONT OFFERTS CHAQUE ANNÉE EN RÉCOMPENSE DE NOTRE ENGAGEMENT DANS LA MAINTENANCE DU RÉSEAU.

Depuis son lancement, sa fréquence de création de blocs a subi plusieurs changements.



Bien que Bitcoin et Ethereum utilisent le même processus de minage, la façon dont les deux systèmes génèrent des blocs diffère.

La fréquence de blocs étant très courte sur Ethereum, il est plus enclin à voir se former des blocs orphelins.

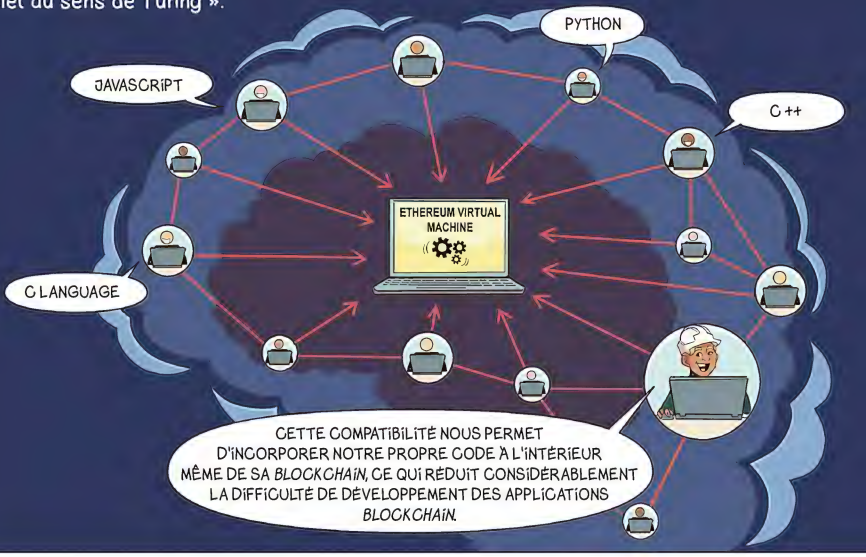


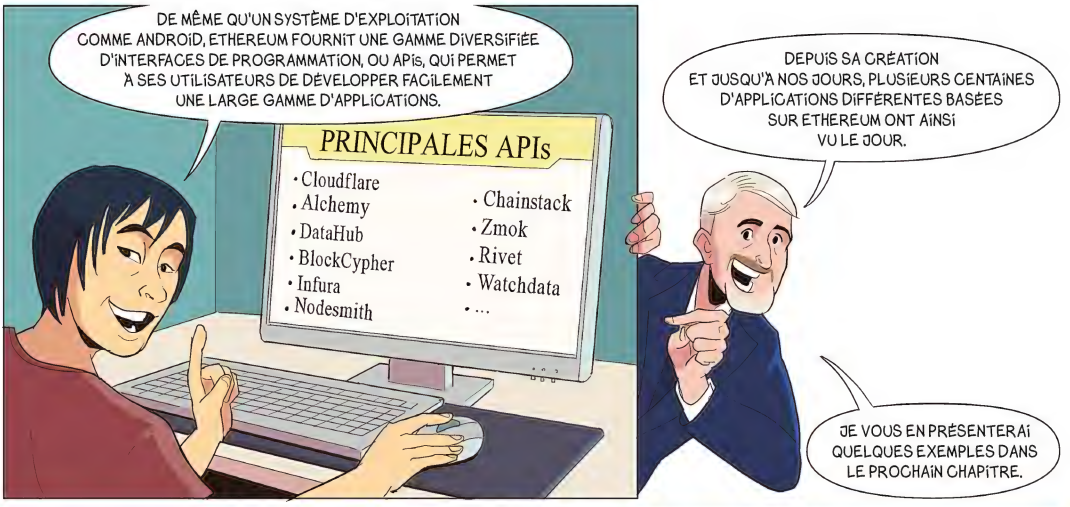
Contrairement à Bitcoin, Ethereum permet l'enregistrement des données de ces blocs, aussi appelés *blocs oncle*, dans la chaîne principale donnant droit à des récompenses.

Une autre différence significative existe entre les deux systèmes : Ethereum est une plateforme de développement *blockchain* PROGRAMMABLE.

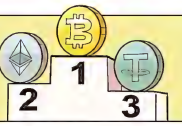
L'EVM est équivalente à un ordinateur mondial décentralisé qui exécute des algorithmes de codage de plus en plus complexes.

Dans ce système, les développeurs peuvent utiliser des langages de programmation de haut niveau de manière compatible. Dans le jargon, on dit qu'un tel système est « complet au sens de Turing ».





Depuis mars 2018, la capitalisation boursière d'Ethereum se maintient au second rang des crypto-monnaies, derrière Bitcoin.



QU'EST-CE QUE EOS ?

Ce système a été lancé en juin 2018 par le développeur Dan LARIMER.

INFOS NEWS

EOS ICO RECORD DANS LE MONDE DE LA CRYPTO-MONNAIE !

Après une campagne de près d'un an, EOS a récolté jusqu'à 4 milliards de dollars !

EOS, FUTUR REMPLAÇANT DU SYSTÈME ETHEREUM ?

De nos jours, plus de 900 millions de jetons EOS sont en circulation.

Comme Ethereum, EOS est une plateforme de développement de *blockchain* programmable et décentralisée.

CERTES, MAIS CONTRAIREMENT À ETHEREUM, ELLE ADOPTE LE MÉCANISME DE CONSENSUS DPoS, QUE J'AI INVENTÉ, AINSI QUE D'AUTRES MÉTHODES TECHNIQUES QUI LA RENDENT HAUTEMENT ÉVOLUTIVE.

	ETHEREUM	EOS
Mécanisme de consensus	PoW	DPoS
Nombre de validateurs des transactions	Totalité des nœuds du réseau	21 nœuds fixes
Vitesse de traitement des transactions	15 par seconde	Jusqu'à 1 million par seconde

AINSI, ELLE A LA CAPACITÉ DE RÉPONDRE RAPIDEMENT À UN ACCROISSEMENT DE LA DEMANDE.

Fin 2022, Ethereum a prévu de lancer une mise à niveau appelée Ethereum 2.0 avec pour objectif d'atteindre les 100 000 transactions par seconde.

Sa grande rapidité permet à EOS de prendre en charge des milliers de programmes commerciaux d'acquisition et de traitement de données appelés DAPP*.

JEUX

RÉSEAUX SOCIAUX

FINANCE

MARKETPLACE

* Pour *data acquisition and processing programs*.

Comme Ethereum, EOS est une *blockchain* publique.

Cependant, leur architecture diffère, car EOS permet aux développeurs de créer librement des chaînes publiques individuelles sans que leurs ressources ne consomment celles des autres.

CELA ÉVITE AINSI L'ENCOMBREMENT DU RÉSEAU LORSQU'UNE CHAÎNE PARTICULIÈRE EST SURCHARGÉE.

ARCHITECTURE ETHEREUM

DAPP 5 %

DAPP 10 %

EVM

ESPACE SATURÉ

DAPP 35 %

DAPP 50 %

ARCHITECTURE EOS

DAPP 5 %

DAPP 10 %

DAPP 35 %

DAPP 50 %

C'EST BEAUCOUP PLUS RAPIDE ET MOINS ÉNERGIVORE !

Grâce à ce système, la réalisation de transactions et l'exécution de contrats intelligents ne nécessite aucun jeton EOS.

SUR ETHEREUM, LES MEMBRES DU SYSTÈME LOUENT UNE MACHINE VIRTUELLE, APPELÉE "EVM", CONTRE DES FRAIS DE TRANSACTION.

SUR EOS, C'EST DIFFÉRENT ! LES TRANSACTIONS SONT GRATUITES, CAR LES DÉTENTEURS DE JETONS SONT PROPRIÉTAIRES DU RÉSEAU AU PRORATA DE LEUR INVESTISSEMENT.

DE PLUS, LORSQUE DES ERREURS SYSTÈME SE PRODUISENT DANS LE RÉSEAU, LA "CONSTITUTION" EOS PEUT ÊTRE UTILISÉE POUR DÉTERMINER SI ELLES SONT DUES À UN BUG, ET POUR ÉVALUER SI LES MESURES CORRECTIVES PRISES PAR LA COMMUNAUTÉ SONT APPROPRIÉES.

ERROR SYSTEM

CONSTITUTION EOS

LES JETONS UTILITAIRES

Aussi appelés *utility tokens*, ces jetons sont construits sur des plateformes *blockchain* telles que Ethereum.

En voici quelques exemples...

AUGUR
Plateforme de marché prédictive

GOLEM
Plateforme de marché pour la puissance de calcul

VECHAIN
Plateforme de gestion *supply chain* de produits de luxe

OMISEGO
Plateforme d'échange décentralisée et ouverte pour les paiements

Chacune de ces applications possède ses propres jetons donnant accès aux produits et services qu'elle fournit.

À ces jetons sont associés des contrats intelligents qui offrent aux utilisateurs une facilité de gestion et d'échange de biens et services de l'économie réelle sur la *blockchain*.

PRENONS L'EXEMPLE DE CE JETON. JE L'AI REÇU EN GUISE DE TITRE DE PROPRIÉTÉ À LA SUITE DE L'ACHAT D'UN VÉHICULE ÉLECTRIQUE.

À PREMIÈRE VUE, IL N'A RIEN D'EXTRAORDINAIRE. MAIS SI VOUS Y REGARDEZ DE PLUS PRÈS, VOUS VERREZ QU'IL RENFERME UN GRAND POUVOIR.

ABONNEMENT BORNES DE RECHARGE ÉLECTRIQUES
Changement de RIB

CARTE GRISE
Changement du propriétaire

ASSURANCE
Modification du contrat

Tous ces transferts de données sont préprogrammés dans le *smart contract* qui met en place AUTOMATIQUEMENT l'ensemble de ces modifications.

Un autre avantage qu'offrent les jetons utilitaires est la possibilité de lever des fonds, rapidement et à moindre coût, lors du lancement d'un nouveau projet, d'une nouvelle entreprise...

... ET MÊME D'UNE NOUVELLE CRYPTO-MONNAIE !

Ce système est appelé *initial coin offering* ou ICO.

CONTRAIREMENT AU SYSTÈME DE FINANCEMENT TRADITIONNEL, PAS BESOIN D'UN PRÊT NI D'ASSOCIÉS.

SON FONCTIONNEMENT REPOSE SUR LE MÊME PRINCIPE QUE CELUI D'UNE CAMPAGNE DE FINANCEMENT PARTICIPATIF.

Le créateur du projet lance la prévente de jetons.

QUI EN VEUT ?

LIVRE BLANC ETHEREUM

Les personnes intéressées acquièrent ces jetons, apportant ainsi une part de financement.

MOI !

MOI AUSSI !

MOI !

MOI !

MOI !

Une fois les fonds levés, chaque partie peut récolter le fruit de son investissement.

PLUS-VALUE.

ACCÈS AUX PRODUITS ET SERVICES DE LA PLATEFORME.

ethereum

L'élément clé du succès d'un projet est la capacité de son initiateur à fédérer un réseau.

PLUS IL Y A DE SOUSCRIPTEURS, PLUS LE JETON SE DÉVELOPPE ET PLUS SA VALEUR AUGMENTE.

POUR LES INVESTISSEURS, LE PARI EST TRÈS RISQUÉ. CERTAINS PEUVENT FAIRE UN BEAU PROFIT, COMME CE FUT LE CAS POUR LES PREMIERS À AVOIR FINANCÉ L'ETHEREUM.

ON A REÇU 2 000 ETH POUR CHAQUE BTC INVESTI*.

OU BIEN TOUT PERDRE SI LE PROJET N'ABOUTIT PAS FAUTE D'UN FINANCEMENT SUFFISANT.

D'UNE MANIÈRE OU D'UNE AUTRE, ON TRINQUE !

Grâce à sa capacité d'implémentation et au système décentralisé de la *blockchain*, les jetons utilitaires peuvent résoudre des problèmes de confiance et de paiements transfrontaliers dans des domaines tels que...

FINANCE

RÉSEAUX SOCIAUX

JETON UTILITAIRE

JEUX

DROITS DE PROPRIÉTÉ INTELLECTUELLE

C'EST D'AILLEURS LE PROJET DE *BLOCKCHAIN* QUI CONNAÎT LA CROISSANCE LA PLUS RAPIDE.

CRYPTO-MONNAIES

PLATEFORMES

JETONS UTILITAIRES

JETONS D'ACTIFS

* Aujourd'hui, il suffit de 14 ETH pour obtenir 1 BTC.

QU'EST-CE QUE LE JETON UTILITAIRE AUGUR ?

Augur a officiellement vu le jour en juin 2015 et représente l'un des premiers projets développés sur la *blockchain* Ethereum.

MES FRÈRES, ICI NOUS POURRONS CONSTRUIRE UNE NOUVELLE PLATEFORME !

BIENVENUE SUR LES TERRES D'ETHEREUM

C'est une plateforme de marché de prédiction et de paris décentralisée qui s'appuie sur la théorie de la « sagesse des foules » pour prévoir les événements futurs.

UN GRAND GROUPE DE PERSONNES EST COLLECTIVEMENT PLUS INTELLIGENT QUE L'INDIVIDU LE PLUS INTELLIGENT DU GROUPE.

Dans le cas d'un sondage traditionnel, le commanditaire peut être confronté à des risques de contrepartie ou de serveurs centralisés.

QUEL TEMPS VA-T-IL FAIRE AUJOURD'HUI ?

L'ORACLE A PRÉDIT QU'IL FERAIT BEAU.

ET MOI, SI J'EN CROIS LA FOULE, JE VOUS PARIE QU'IL VA PLEUVOIR !

MINCE, J'AI MAL INTERPRÉTÉ LES SIGNES !

En utilisant la « sagesse de la foule », Augur réduit toute subjectivité et garantit ainsi des prévisions rationnelles.

De plus, les « prédicteurs » utilisent des jetons Augur pour parier et prédire.

CEUX QUI PRÉDISENT CORRECTEMENT GAGNENT LES JETONS DE CEUX QUI ONT PERDU LE PARI.

NOUS AVONS DONC UN INTÉRÊT TRÈS PERSONNEL À FOURNIR DES PRÉDICTIONS QUI S'AVÈRENT LES PLUS JUSTES POSSIBLE.

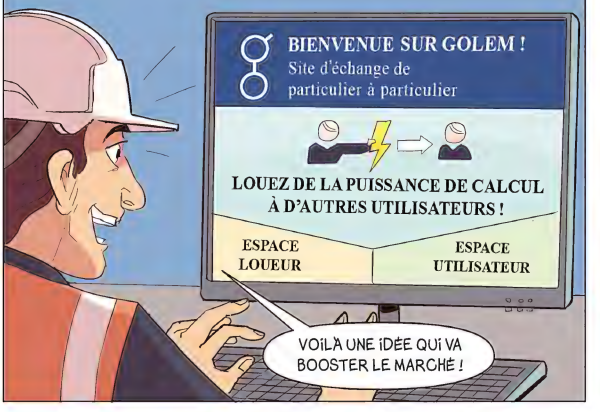
C'est pourquoi les prédictions d'Augur sont perçues comme étant les plus proches de la vérité.

Grâce à la portée mondiale de la *blockchain*, Augur a pu étendre son marché sur tout le globe.

JE PRÉDIS QUE NOTRE AVENIR SERA GLORIEUX !

QU'EST-CE QUE LE JETON UTILITAIRE GOLEM ?

Golem est la première plateforme construite sur Ethereum qui permet l'échange de puissance de calcul excédentaire entre particuliers.



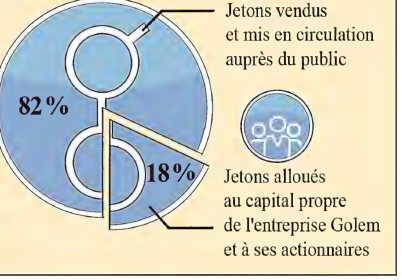
En effet, le marché de la puissance de calcul était jusqu'à présent en situation de quasi-monopole avec peu d'acteurs qui en tiraient des bénéfices élevés, ce qui provoquait...

Grâce à son fonctionnement décentralisé, Golem rend ce marché accessible à tous et aide ainsi à baisser les prix.

En utilisant la technologie de la *blockchain*, Golem connecte des ordinateurs partout dans le monde, établissant une économie de partage de la puissance de calcul.

Lorsque les utilisateurs ont besoin de puissance de calcul, ils doivent fournir des jetons Golem aux fournisseurs comme paiement.

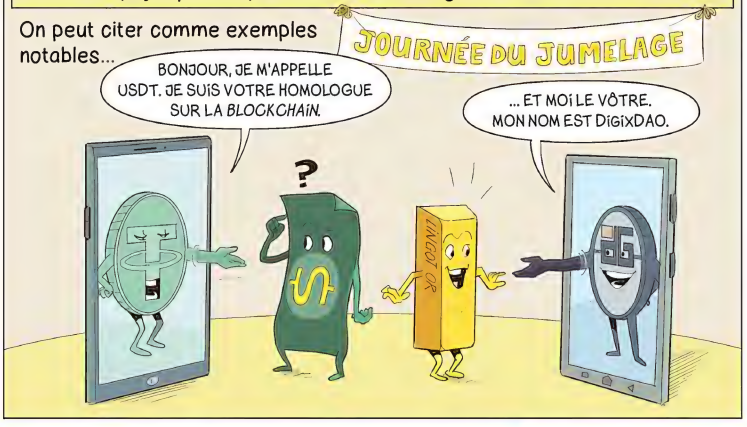
Un milliard de jetons GNT sont en circulation.



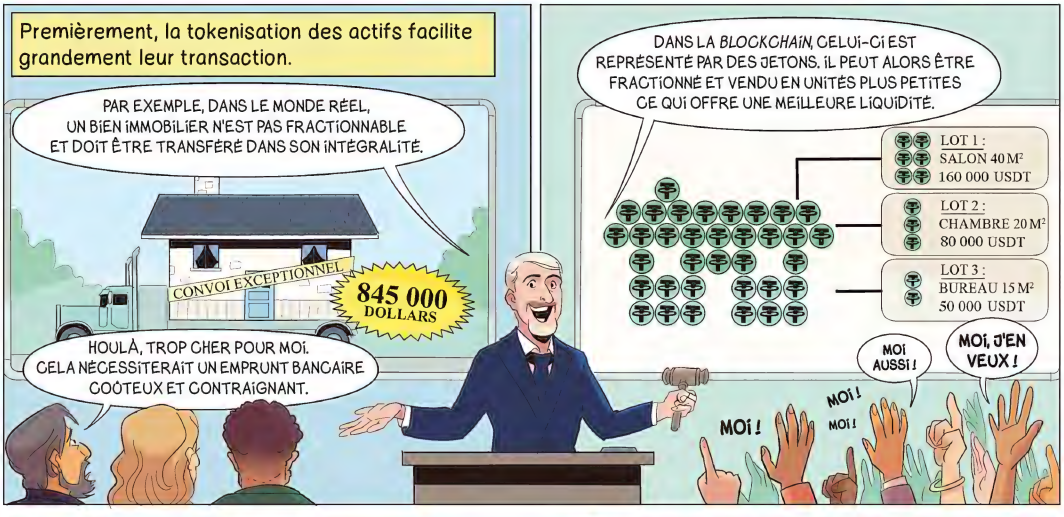
LES JETONS D'ACTIFS

Aussi appelés *asset tokens*, ces jetons sont l'équivalent numérique des actifs physiques et permettent leur enregistrement sur la *blockchain*.

On peut citer comme exemples notables...



Premièrement, la tokenisation des actifs facilite grandement leur transaction.



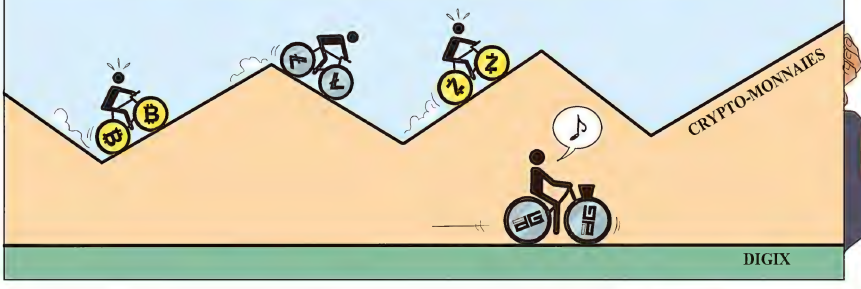
Deuxièmement, elle facilite la sécurité de leur détention.

Des actifs malléables tels que l'or peuvent être endommagés lors de transactions physiques, et leur valeur ainsi altérée.

Avec la représentation par jetons, aucun transfert physique d'actifs n'est requis, ce qui garantit leur sécurité et leur état de préservation.

QU'EST-CE QUE LE JETON D'ACTIFS DIGIX ?

Au même titre que l'or dans le monde réel, ces jetons (sous l'acronyme DGX) offrent une valeur refuge dans l'univers très volatil des crypto-monnaies.



Par exemple, si vous voulez vendre un lingot d'or de 1 kg de manière traditionnelle...

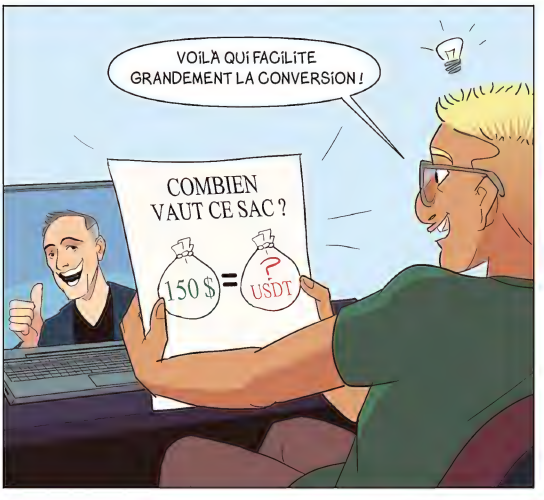
Située à Londres et à Singapour, la LBMA est l'organisation mondiale qui supervise et encadre les marchés de l'or et de l'argent.

Ce fractionnement numérique augmente considérablement la liquidité de votre allocation d'actifs en métal précieux.

À l'inverse, si vous souhaitez récupérer votre lingot d'or, tout ce dont vous avez besoin est de rassembler les jetons requis en échange du certificat, vous permettant alors de récupérer l'or.

QU'EST-CE QUE LE JETON D'ACTIFS USDT ?

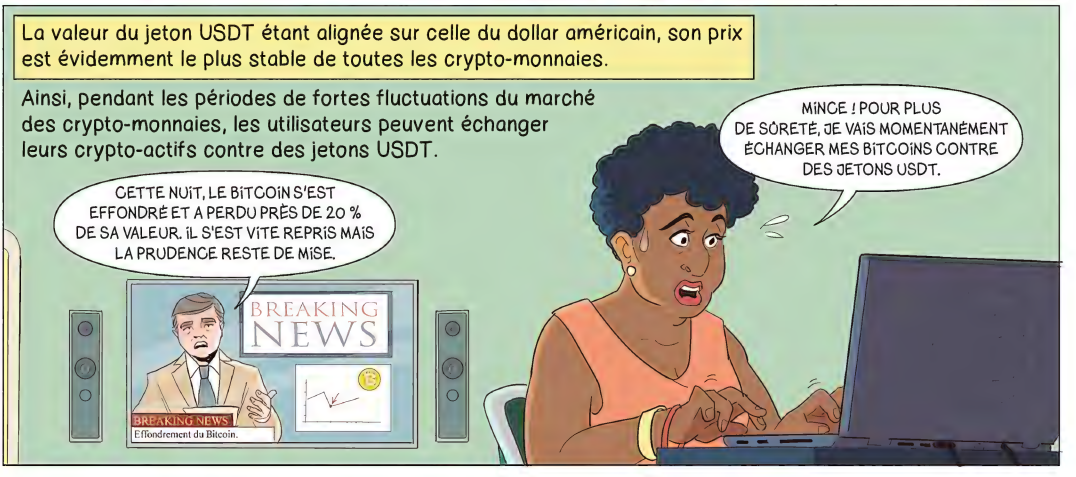
Ce jeton adossé au dollar américain est émis par l'entreprise Tether Limited.



Échanger des devises fiat en jetons USDT est également très simple.

La valeur du jeton USDT étant alignée sur celle du dollar américain, son prix est évidemment le plus stable de toutes les crypto-monnaies.

Ainsi, pendant les périodes de fortes fluctuations du marché des crypto-monnaies, les utilisateurs peuvent échanger leurs crypto-actifs contre des jetons USDT.

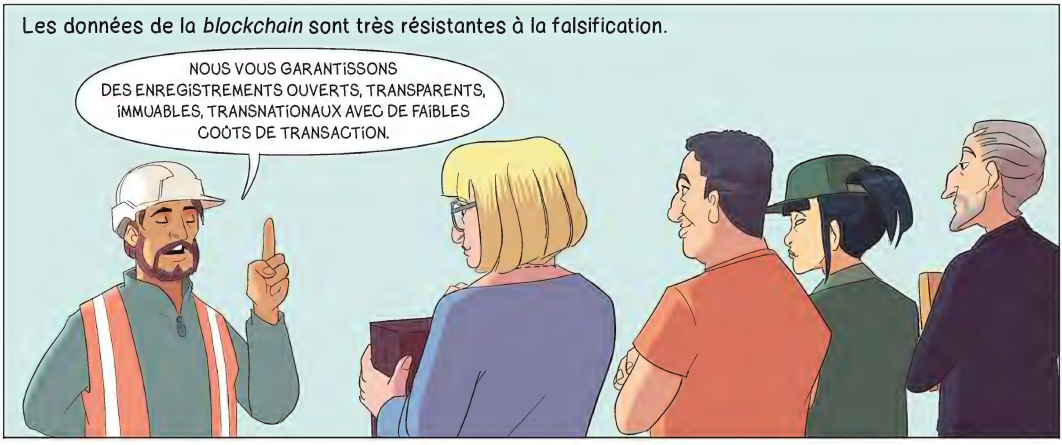


CHAPITRE 9

POTENTIEL DE LA BLOCKCHAIN

LA *BLOCKCHAIN* PEUT-ELLE CHANGER LE MONDE COMME INTERNET L'A FAIT ?
Tous deux sont considérés comme des percées technologiques qui ont inauguré une nouvelle ère.
UN PETIT PAS POUR L'HOMME...
... UN GRAND PAS POUR L'HUMANITÉ !
WWW
REGISTRE
Internet a rendu la TRANSMISSION D'INFORMATIONS décentralisée possible.
GRÂCE À CE SYSTÈME, ON PEUT DIFFUSER OU RECEVOIR DES INFORMATIONS TRÈS RAPIDEMENT, OÙ QUE L'ON SOIT DANS LE MONDE.
La transmission, par exemple d'un document, Word *via* Internet, est en fait une duplication d'informations, qui donne à toutes les parties une copie de l'information originale.
COPIE
La *blockchain*, quant à elle, a rendu possible la TRANSMISSION DE VALEURS décentralisée.
Contrairement à Internet, le système ne duplique pas mais effectue un transfert de propriété.
ET HOP, C'EST ENVOYÉ !
TRANSACTION EFFECTUÉE !
Débit : - 0,05 BTC
UNE FOIS TRANSFÉRÉS DANS LA *BLOCKCHAIN*, LES JETONS N'APPARTIENNENT PLUS À L'EXPÉDITEUR MAIS AU DESTINATAIRE.
COMPTE CLIENT BITCOIN
Crédit : + 0,05 BTC

Les données de la *blockchain* sont très résistantes à la falsification.



Grâce à cela, ce système convient aux scénarios où la confiance ne peut pas être établie, ou trop coûteuse à implémenter, ou encore lorsque l'on souhaite pouvoir contourner des intermédiaires.
De nos jours, les secteurs d'activité dans lesquels la *blockchain* peut être utilisée sont extrêmement divers.

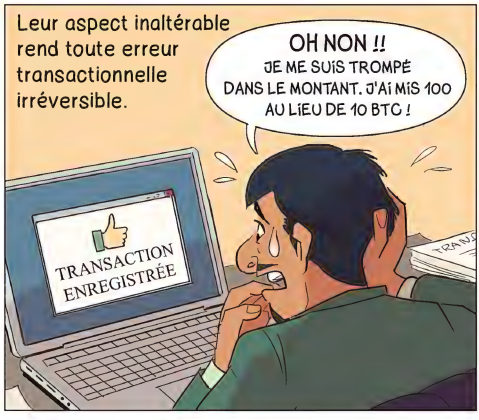
De fait, elle peut être utilisée pour établir la confiance entre les institutions et changer le monde avec la numérisation de la valeur, au même titre qu'Internet l'a fait avec la numérisation de l'information.

QUELS SONT LES INCONVÉNIENTS DE LA *BLOCKCHAIN* ?

Il existe de nombreux aspects positifs de la *blockchain*, mais ses limitations sont également évidentes.

Les informations qui y sont enregistrées étant publiques et transparentes, cela signifie qu'une fois que le compte d'un individu est connu...

Leur aspect inaltérable rend toute erreur transactionnelle irréversible.



Le caractère décentralisé de la *blockchain* oblige chaque nœud individuel à effectuer des vérifications et donc à tenir un registre complet.

Dans le même temps, comme il n'y a pas d'organisation centrale pour conserver une clé privée, en cas de perte...

Enfin, l'efficacité d'un réseau décentralisé à atteindre un consensus entre les nœuds est très limitée, et un tel système a donc beaucoup de mal à être aussi rapide que les systèmes de paiement centralisés.

LES GRANDES ORGANISATIONS AUTOUR DE LA BLOCKCHAIN

LISTE RÉPERTORIÉE DEPUIS 2017

LE NOMBRE FAIT LA FORCE !

Au début de son développement, de nombreuses entreprises et organisations ont formé des alliances et des consortiums pour partager les connaissances de leurs recherches et explorer son potentiel.

R3 CEV
RÉUNIT PLUS DE 40 INSTITUTIONS FINANCIÈRES

r3.

HYPERLEDGER
DIRIGÉ PAR LA FONDATION LINUX

HYPERLEDGER

THE LINUX FOUNDATION

Moscou

RUSSIA BLOCKCHAIN ALLIANCE
AUSSI APPELÉE RUSSIAN R3

CHINALEDGER

CHINALEDGER ALLIANCE
REGROUPE 11 BOURSES

GBA
GOVERNMENT BLOCKCHAIN ASSOCIATION

CRYPTO-NEWS – Octobre 2022

« La GBA a pour vocation de nourrir la relation entre instances gouvernementales, régulateurs et les entreprises du secteur privé au sujet des applications de la *blockchain*. »

Gerard DACHE
Directeur exécutif

GBA

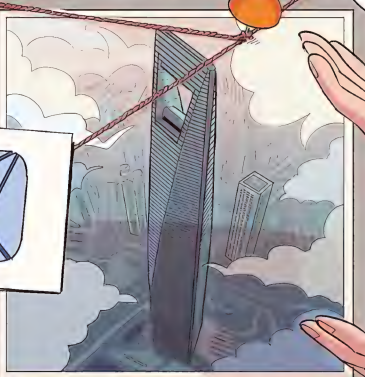
ZHONGGUANCUN BLOCKCHAIN INDUSTRY ALLIANCE
SITUÉE DANS LA "SILICON VALLEY" CHINOISE

BCMFIA
BCMFIA

La Blockchain Micro-Finance Industry Alliance cherche à intégrer la *blockchain* dans la microfinance.

FISCO
CONSTITUÉ DE 25 INSTITUTIONS FINANCIÈRES

FISCO 金链盟
Financial Blockchain Shenzhen Consortium



Située dans le centre financier de Shanghai

LJZ-FIN
LUJIAZUI BLOCKCHAIN FINANCE DEVELOPMENT ALLIANCE

LE POTENTIEL DE LA *BLOCKCHAIN* EST INFINI LORSQUE LES TALENTS ET LES ORGANISATIONS SE RÉUNISSENT POUR INSPIRER ET ENCOURAGER SON UTILISATION ET SON DÉVELOPPEMENT.

Olivier Bossard est professeur de finance à HEC Paris, où il dirige le Master Finance depuis 2016.
Passionné par l'enseignement, il innove et expérimente les supports pédagogiques pour partager ses connaissances avec le grand public : podcasts, tweets, cours et vidéos en ligne.
En 2019, le « prof-youtubeur » aux 58 millions de vues reçoit le prix du Meilleur professeur d'HEC Paris.
En 2019, son *Introduction à la Finance avec Largo Winch*, illustrée par Philippe Francq, nous fait découvrir le fonctionnement de la bourse et des marchés financiers. Dans la foulée, en 2020, Olivier est nommé conseiller économique de la magistrale exposition *Largo Winch, aventurier de l'économie*, qui ouvre ses portes à CitéCo, le Musée de la Banque de France.
En tandem avec Maud Rivière, il s'attèle à un nouveau défi : démystifier le Bitcoin et la *blockchain* !

Diplômée de l'École supérieure de communication visuelle Brassart, **Maud Rivière** travaille pendant 10 ans en entreprise en tant que graphiste. Durant cette période, elle développe en parallèle une de ses passions, l'illustration...
C'est en 2014 qu'elle saute le pas et décide de lier ces deux activités en devenant graphiste et illustratrice indépendante.
Au fil des projets qui lui sont confiés, elle jongle entre les supports (graphisme, illustration, BD) et entre les styles (jeunesse, cartoon, réaliste).
Adepte de la simplification visuelle, Maud Rivière aime apprendre et comprendre pour mieux transmettre.
Ainsi, lorsque Olivier Bossard lui propose en 2021 de collaborer sur le projet de *La Grande Aventure du Bitcoin et de la blockchain*, elle accepte cette nouvelle opportunité.
Sa philosophie ? « Un petit dessin vaut mieux qu'un long discours ! »

POSTFACE

Le Bitcoin… Quelle incroyable épopée du début du XXIe siècle !
En 2013, le Bitcoin existait déjà depuis quatre ans, et je découvrais, sceptique, ce concept de monnaie numérique basé sur la cryptographie. Un bitcoin valait alors à peine 300 dollars.
Cinq années plus tard, subjugué par la technologie sous-jacente, la fameuse *blockchain*, je décidais d'écrire la trame de ce livre, alors que le cours du Bitcoin avait déjà été multiplié par 50 !
Depuis 2021, que Maud et moi travaillons à la mise en images de cette aventure, il a encore triplé, dépassant les 50 000 dollars sous l'effet d'une spéculation effrénée… pour finalement redescendre sous la barre des 20 000 dollars. Et les montagnes russes continuent !

Le Bitcoin a hystérisé les investisseurs, il a fait et défait les fortunes, et aussi fait trembler les banques centrales et les gouvernements. Certains lui voyaient un brillant avenir, dépassant les 100 000 dollars, mais je continue d'irriter ses fans en réaffirmant que le Bitcoin en tant que tel n'a aucun avenir et que sa valeur retombera à zéro. Pour quelles raisons ? Le protocole du Bitcoin ne permet pas une adoption de masse car il est outrageusement énergivore, que sa mise à l'échelle est compliquée et qu'il ne peut rivaliser avec les systèmes de paiement en ligne traditionnels.

Alors, pourquoi tant de passions, d'enthousiasme, et pourquoi cet ouvrage, me direz-vous ?
Parce que, au-delà du rêve libertaire des cypherpunks, au-delà de la bulle spéculative, le Bitcoin reste le premier cas d'école d'une nouvelle technologie, la *blockchain* qui, elle, est promise à un avenir incroyable ! Des registres distribués aux contrats intelligents, la technologie *blockchain* va rentrer dans nos sociétés au même titre qu'Internet a révolutionné le monde de l'information.
Alors oui, le Bitcoin va mourir mais son aventure extraordinaire marque le début d'une nouvelle révolution numérique que nul ne peut ignorer.

Voici bientôt dix ans que j'étudie quotidiennement pendant plusieurs heures chaque soir pour tenter de comprendre en profondeur cette technologie en perpétuelle (r)évolution. Et voici plus d'un an que Maud et moi avons relevé le défi de vous raconter cette fabuleuse histoire. Ainsi nous vous proposons, à travers des mots simples et des images pétillantes, de découvrir avec humour et pédagogie cette incroyable épopée.

Si après avoir refermé ce livre vous comprenez enfin le concept du Bitcoin et de la *blockchain*, nous aurons gagné notre pari ! Si de plus vous vous êtes divertis et avez envie d'aller encore plus loin dans cette découverte, alors, vous aurez comblé nos espérances !

OLIVIER BOSSARD

POUR ALLER PLUS LOIN

***L'Internet de l'argent. Recueil de conférences*, volumes 1, 2 et 3, d'Andreas Antonopoulos, Éditions Dicoland.**
Andreas Antonopoulos est bien connu au sein de la communauté Bitcoin pour être l'un des ambassadeurs les plus déclarés du monde. Il possède la capacité de décomposer ce sujet difficile en termes simples, rendant ainsi la notion du Bitcoin intelligible pour un profane.

Accessibilité : tous publics.

***L'Étalon-bitcoin : l'alternative décentralisée aux banques centrales*, de Saifedean Ammous, Éditions Dicoland.**
Ce livre met en évidence la proposition de valeur du Bitcoin du point de vue monétaire. Il s'appuie sur la littérature économique et l'école autrichienne d'économie tout particulièrement, en opposition à l'école keynésienne.

Accessibilité : tous publics, mais ne décevra pas pour autant les académiques et universitaires de haut rang.

***Digital Gold*, de Nathaniel Popper, Éditions Penguin.**
Une galerie de portraits des pionniers du Bitcoin, de leurs succès, de leurs défaites. Hal Finney, Mark Karpelès, Roger Ver, Erik Voorhees, les jumeaux Winklevoss… Ils sont tous là. Cet ouvrage se dévore comme un thriller haletant.

Accessibilité : tous publics mais en anglais.

***De la blockchain à crypto-investisseur*, de Jens Helbig, Éditions KLHE finance.**
Jens Helbig s'adresse aux investisseurs en herbe qui souhaitent investir dans le Bitcoin, Ethereum, Ripple et autres crypto-monnaies. Bien que ne cautionnant pas du tout de tels investissements spéculatifs, je reconnais à Helbig la lisibilité du propos et la qualité des conseils pratiques.

Accessibilité : tous publics, à condition de savoir limiter ses investissements à la hauteur du raisonnable.

***Introduction à la finance avec Largo Winch*, de Olivier Bossard, illustrations de Philippe Francq, textes originaux de Jean Van Hamme et Éric Giacometti, Éditions Dupuis.**
Au-delà du Bitcoin, pour comprendre plus globalement la finance 2.0 du XXIe siècle, en compagnie de Largo Winch, beau gosse et milliardaire humaniste. Une plongée vertigineuse dans les arcanes de la finance moderne.

Accessibilité : tous publics.

***Au cœur du Bitcoin. Programmer la blockchain ouverte*, d'Andreas Antonopoulos, Éditions O'Reilly.**
Cet ouvrage très technique d'Antonopoulos permettra aux fans de comprendre en profondeur la technologie Bitcoin et même de programmer leur propre blockchain. Je l'ai fait !

Accessibilité : pour programmeurs avertis.

Cet ouvrage représente avant tout pour moi une belle et grande aventure humaine dont je tiens à remercier chaque participant. Alors MERCI…

À Olivier, pour m'avoir ouvert les portes de cet univers et pour ta confiance.

À toute l'équipe Delcourt, d'avoir rendu cette aventure possible.
Alix, Lorène et Adèle, mille mercis pour vos précieux conseils et votre bienveillance !

À toi qui tiens ce livre entre tes mains, pour l'attention que tu lui porteras.

À Christophe, Y-C., Steph, Aude et Annabelle, qui sans s'en rendre compte, m'ont permis d'arriver jusque-là.

Et enfin à mes deux amours, pour leur patience et leur soutien au quotidien.

Maud Rivière

Merci à tous ceux qui m'ont accompagné tout au long de mon voyage initiatique dans ce monde incroyable de la Finance 3.0.

À commencer par les pionniers d'avant l'heure, mes professeurs de l'Université nationale de Yokohama, où j'ai découvert la cryptographie, les réseaux de neurones et l'intelligence artificielle … il y a plus de 30 ans maintenant !

À mes étudiants passionnés d'HEC Paris, de l'Université de Tsinghua et d'Hitotsubashi.

À Éloïc et Jacques pour leur confiance.

À Maud, enfin et surtout, qui a su par ses dessins et ses idées géniales rendre un sujet ardu accessible à tous !

Olivier Bossard

Du même scénariste, aux éditions Dupuis :
• *Introduction à la finance avec Largo Winch* - illustrations de P. Francq, textes originaux de J. Van Hamme et É. Giacometti

Éditrice : Alix de Sanderval

© 2022 Éditions Delcourt

Tous droits réservés pour tous pays
Dépôt légal : septembre 2022. ISBN : 978-2-413-05288-3

Conception graphique : Studio Delcourt/Soleil

www.editions-delcourt.fr